SnapGear™ VPN Router Family
User Manual

Rev: May 30, 2002

7984 South Welby Park Drive #101
Salt Lake City, Utah 84084
Tel: 801-282-8492
Fax: 801-282-8496

1. Introduction 1

Terminology 2

Document Style 5

Installing and configuring the SnapGear VPN Router 6

The SnapGear VPN Router 7

SnapGear VPN Router features 9

2. Getting Started 11

New Networks 12

Setup Wizard 13

System requirements 13

Configuring the SnapGear VPN Router on your network 13

Initial setup using Linux 16

SnapGear Quick Setup Wizard 18

Configuring the PCs on your network 22

3. Connect to the Internet 24

Physically connect modem device 24

Select Internet connection 25

Configure PCs to use SnapGear VPN Router Internet gateway 28

Establishing the connection 28

4. Dial-in server configuration 30

Dial-in setup..... 31

Dial-in user accounts..... 34

Remote user configuration 38

5. Network Configuration 48

IP Configuration..... 48

Advanced IP Configuration 51

DHCP Server..... 53

Advanced Networking 54

6. Firewall 56

Incoming Access 56

Outgoing Access 59

Firewall Rules..... 61

Intruder Detection and Blocking..... 62

7. Virtual Private Networking 64

PPTP client setup..... 66

PPTP server setup 68

IPSec Setup 82

IPSec Interoperability 87

8. System 88

Time Server 88

Password 88

Diagnostics 88

Advanced 89

RESET button 89

9. Technical Support 90

Appendix A – LED Status Patterns 91

1. Introduction

This chapter provides an overview of the SnapGear VPN Router's features and capabilities, and previews how to install and configure your SnapGear VPN Router.

The SnapGear VPN Router enables small to medium-sized businesses to securely interconnect computers on the office network to the Internet. The SnapGear VPN Router has all the features a business needs to take full advantage of the Internet. Whether you are connecting to the Internet for the first time or looking for a cost-effective and safe VPN solution, the SnapGear VPN Router will meet your needs.

The SnapGear VPN Router simply and securely interconnects your network to the Internet through a robust embedded firewall. Shielded behind a NAT gateway, your office computers are protected from outside threats. The SnapGear VPN Router filters and inspects packets of data to prevent unauthorized Internet applications from accessing your network.

The SnapGear VPN Router provides your network with a virtual private network (VPN) server. A VPN enables remote workers or branch offices to securely access your company network to send and receive data at a very low cost. With the SnapGear VPN Router, you can now remotely access your office network securely through the Internet. Additionally, the SnapGear VPN Router is able to connect as a client to external VPNs.

With the SnapGear VPN Router, everyone on your office LAN can access the Internet through the one connection. Your entire network can log on to the Internet using only one ISP account through the one analog modem, DSL, or ISDN line, eliminating the need for a separate connection and ISP charge for each individual user. With a dial-in modem connected to your SnapGear VPN Router, your remote staff can also securely direct-dial into your office network.

This manual details how to take advantage of the features of your SnapGear VPN Router – including setting up a VPN, a secure firewall and an Internet connection. It also details how to set up the SnapGear VPN Router on your existing or new network. This is done through the web configuration interface.

Installing your SnapGear VPN Router into a well-planned network is quick and easy. However, network planning and design is outside the scope of this manual. Please take some time to plan your network prior to installing your SnapGear VPN Router.

Terminology

Some commonly used terms that you will find in this document are as follows:

ADSL	Asymmetric Digital Subscriber Line. A technology that allows for high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mb/s when receiving data and between 16 and 640 Kb/s when sending data.
BOOTP	Bootstrap Protocol is a protocol that lets a network user automatically receive an IP address and have an operating system boot without user involvement. BOOTP is the basis for the more advanced DHCP.
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
DNS	Domain Name System. This system allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking.
Ethernet	A physical layer protocol based upon IEEE standards.
Extranet	A private network that uses the public Internet to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company’s intranet.
Firewall	A network gateway device that protects a private network from users on other networks. Typically, a firewall is installed to allow users on an intranet access to the public Internet without allowing all public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.

IDB	Intruder Detection and Blocking. A feature of your SnapGear VPN Router that detects connection attempts from intruders and optionally blocks all further connection attempts from the intruders' machine.
Internet	A worldwide system of computer networks - a public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP.
Intranet	A private TCP/IP network contained within an enterprise.
IPSec	Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically based security at the IP layer, thus offering protection for all network communications.
LAN	Local Area Network.
LED	Light-Emitting Diode.
MAC Address	An Ethernet address set by the manufacturer.
Masquerade	The process by which a gateway on the local network modifies outgoing packets to replace the source address of these packets with its own IP address. In this way, all IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network.
NAT	Network Address Translation. The translation of an IP address used on one network to another IP address known on another network.
Net Mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.
NTP	Network Time Protocol (NTP) is used to synchronize clock times in a network of computers.
PAT	Port Address Translation. The translation of a port number used on one network to another port number known on another network.

PPP	Point-to-Point Protocol. A networking protocol designed for simple links between two peers.
PPPoE	Point to Point Protocol over Ethernet. A protocol for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.
PPTP	Point-To-Point-Tunneling-Protocol. This is a protocol developed by Microsoft™ that is now popular for VPN applications. While generally not considered as secure as IPSec it is considered "good enough" technology, especially since Microsoft responded to a number of flaws in the original implementations.
Road Warrior	A remote machine that does not have a fixed IP address.
Router	A network device that moves packets of data. Differs from a hub or switch in that a router usually is "intelligent" enough to know where final destinations should be and how to get the packets there.
Subnet Mask	See "Net Mask".
Switch	A network device that is like a hub, but much smarter. Although not a full router, a switch understands, to some degree, the routing of Ethernet packets and adds efficiency to a LAN by utilizing bandwidth more effectively.
TCP/IP	Transmission Control Protocol / Internet Protocol – the basis of Internet communications!
TCP/IP Address	An address of the form nnn.nnn.nnn.nnn is the fundamental addressing form of the Internet.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. Most commonly known as Category 5 or CAT 5, representing a type of Ethernet cable that can operate up to 100Mb/s.

VPN	Virtual Private Networking is the concept of having two locations able to communicate securely and effectively, usually across a public network such as the Internet. Three key traits of VPN technology are: privacy (nobody else can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody else can tamper with your messages/data).
WAN	Wide Area Network.
WINS	Windows Internet Naming Service (WINS) manages the association of workstation names and locations with Internet Protocol addresses.

Document Style

Warnings: *Where there is something that you should take particular note of, warning text like this will appear.*

Bold text in procedures indicates text that you type or the name of a screen object (such as a menu or button).

Installing and configuring the SnapGear VPN Router

Instructions for installing and configuring your new SnapGear VPN Router on your network are contained in this manual. The basic steps and related chapters are as follows:

Step	**See chapter:**
1. Interconnect the SnapGear VPN Router and PCs on a local area network.	Chapter 2, Getting Started
2. Connect the telecommunications hardware/modem (for dial in/dial out internet access).	Chapter 3, Connect to the Internet
3. Set up the network IP addresses and firewall.	Chapter 2, Configuring the SnapGear VPN Router on your network
4. Set up Internet hardware and Internet account and connect to the Internet.	Chapter 3, Connect to the Internet
5. Set up users' security dial-in/dial out/VPN.	Chapter 4, Dial-in server configuration Chapter 7, Virtual Private Networking Chapter 6, Filtering and Security Groups

The SnapGear VPN Router

The following items will have been included with your SnapGear VPN Router:

- Power adapter
- Installation CD
- Printed Quick Install guide
- Cabling:
  - 1 x normal UTP cable – *blue*
  - 1 x "cross-over" UTP cable – (either *gray* or *red*) With the LITE+ you will instead receive two straight through cables (*blue*).

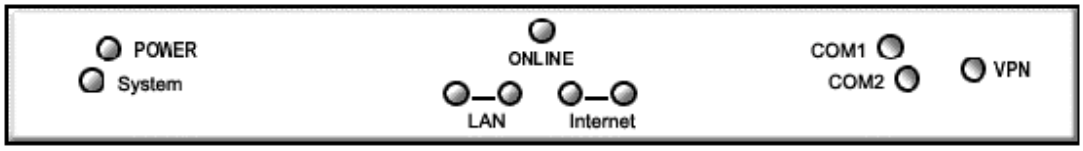


Figure 1.1 SnapGear SOHO+/PRO front panel LEDs

As shown above, the front panel contains 'status' LEDs. You will also find status LEDs on the rear panel.

Label	Activity	Description
POWER / PWR	On	Power is supplied to the SnapGear VPN Router.
System / SYSTEM	Flashing	System will flash once every second while the SnapGear VPN Router is operating correctly.
	On	If System is on and not flashing, an operating error has occurred. In this case the other LEDs form a diagnostic pattern to indicate what has failed. More information on these patterns can be found in
Online / ONLINE	On	Indicates that a valid Internet connection is present.

COM 1, 2	Flashing	For either of the SnapGear VPN Router COM ports, these LEDs indicate receive and transmit data.
VPN	On	Virtual Private Networking is enabled.

The rear panel contains connector ports for LAN (*LAN*) and modem (*COM1*, *COM2*), LAN 10BaseT status LEDs, WAN 10BaseT status LEDs, a reset button and power inlet. The upper LEDs represent "Link" condition, where a cable is connected correctly to another device (such as a cable modem). The lower light represents "Activity" as per the front panel.

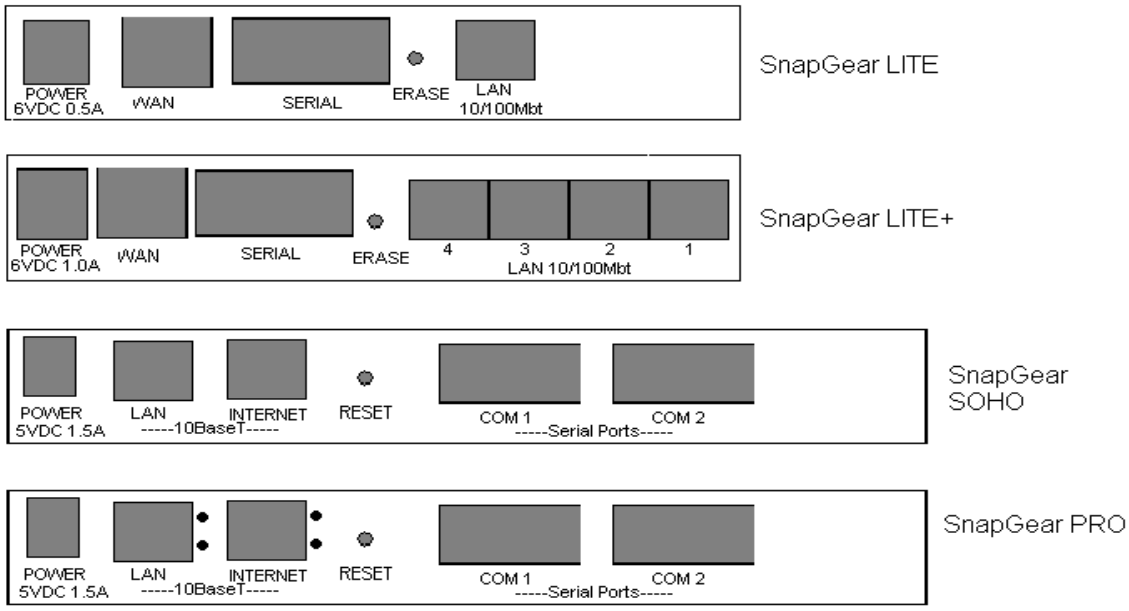


Figure 1.2 SnapGear VPN Router back panels

The SnapGear VPN Router interconnects as shown below. In the case of the SnapGear LITE+ a secondary hub/switch is not required as the unit provides a 4-port Ethernet switch.

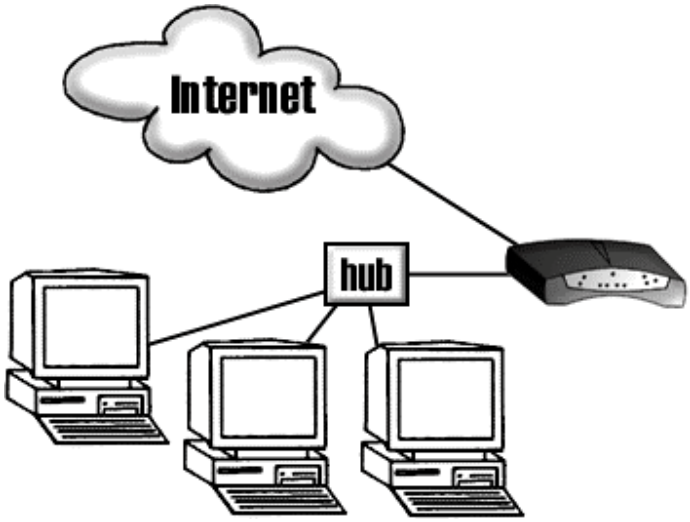


Figure 1.3 Network interconnections

SnapGear VPN Router features

Software features

- Network Address Translation (NAT) firewall, which isolates the LAN from the Internet and offers network access control and filtering
- DHCP server and client, which ensures simple, flexible IP network configuration
- PPTP VPN server that provides communications to remote users running standard Windows VPN client software
- PAP, CHAP, MSCHAPv2, RADIUS and TACACS+ tunnel authentication (RFC1334, RFC1994)
- Transparent tunnel support for PPTP. IPSec pass through.
- Dial-in remote access with PAP, CHAP, MSCHAPv2, RADIUS and TACACS+ authentication
- Dial-on-demand for outgoing Internet connection
- Wizard setup and browser based management and configuration
- Flash upgradeable firmware that allows latest protocols and security software to be downloaded and installed over the web
- Connect Windows PCs, Macintoshes, Linux and Unix workstations – anything that talks IP – to the Internet

Internet link

- Connect to the Internet with an external cable modem, DSL, dial-up or ISDN modem
- Serial ports (*COM1*, *COM2*) connect to the Internet through an external modem or ISDN T/A (LITE/LITE+ models have a single serial port)
- 10baseT Ethernet port (*Internet*) connects to the Internet through a cable or ADSL modem
- Front panel serial status LEDs (for TXD/RXD)
- Online status LEDs (for Internet/VPN)
- Rear panel Ethernet LEDs (Link Transmit/Receive)

LAN link

For the SnapGear SOHO+ and PRO models:

- 10BaseT LAN port to connect to local network Ethernet hub
- Rear panel Ethernet LEDs (Link Transmit/Receive)

For the SnapGear LITE and LITE+ models

- 10/100BaseT LAN port to connect to local network

Dial-in Connection

- For SnapGear SOHO+ and PRO, external modems may be attached to the serial ports for dial-in connection

Environmental

- External power adaptor (voltages/current depend on individual models)
- Front panel status LEDs: Power Test
- Operating temperature 0° C to 40° C
- Storage temperature -20° C to 70° C
- Humidity 0 to 95%, non-condensing

2. Getting Started

The SnapGear VPN Router provides a secure, simple gateway to connect PCs and other devices on your local network to the outside world. This chapter walks you through connecting the SnapGear VPN Router to your LAN. The procedures in this section are similar to those in the *SnapGear Quick Install Guide*, which you may prefer to use if you are in a hurry.

Using an Ethernet cable, connect the SnapGear VPN Router's LAN Ethernet port (marked LAN) to a spare port on the existing network hub. At this stage do not apply power to your SnapGear VPN Router.

SnapGear VPN Router comes with an inbuilt DHCP server that can automatically assign IP addresses to other devices on the network. If you have an existing network, there may already be an active DHCP server. Additionally, the PCs and devices on the network will already have their IP addresses assigned. So, to make installation in existing networks simpler, SnapGear VPN Router ships without an initial IP address of its own and without the DHCP server activated.

Note

The following steps detail the initial setup procedure for networks with at least one Windows workstation. If you wish to perform the setup procedure using a Linux box, skip to Initial Setup using Linux *later in this chapter.*

New Networks

If you do *not* have an existing LAN, follow these steps to get started:

1. Install the hub according to its instructions (LITE+ has an advanced Ethernet switch making a hub unnecessary for small networks).

2. Install an Ethernet adapter and software driver in at least one of the PCs to be networked.

3. You will have to assign your PC an IP address in order to be able to configure the SnapGear VPN Router on the network. From the **Start** menu, select **Settings, Control Panel, Network** and click on the **Configuration** tab (or **Protocols** if using NT).

4. Ensure that the TCP/IP networking protocol is installed. If not, click **Add** (then **Protocol** if using Windows 95/98, **Microsoft** then **TCP/IP**). Your PC will then reboot.

5. Highlight **TCP/IP** (this is followed by your Ethernet adapter's name if using 95/98) and click **Properties.**

6. In the IP Address pane, select **Specify an IP Address**. Private network addresses should be taken from the ranges:

```
 10.0.0.0 - 10.255.255.255  (10/8 prefix)
172.16.0.0 - 172.31.255.255  (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
```

7. Enter this into the **IP Address** field followed by a number (1-255) to identify your PC, e.g. *10.0.0.45*. You may have to reboot at this point.

8. Connect both the SnapGear VPN Router and the PC to the hub and continue with the steps below. When you reach the final stages of setting up your SnapGear VPN Router, it is recommended that you take advantage of using the SnapGear VPN Router as a DHCP server and set up the PCs on your network to receive TCP/IP configuration information dynamically.

Setup Wizard

SnapGear VPN Router ships with a Windows installation program, **SnapGear Setup Wizard**. If you are using statically pre-assigned IP addresses on your network (i.e. no active DHCP server, a static network), Setup Wizard will help assign an IP address to the SnapGear VPN Router. On DHCP enabled, or dynamic, networks, Setup Wizard will locate the IP address your SnapGear VPN Router has been assigned. It also gives you the option of configuring the Internet connection setup and changing the SnapGear VPN Router's password.

System requirements

Setup Wizard can be run from any PC on the network that is running Windows 2000, Windows XP, Windows ME, Windows NT 4 or Windows 95/98. If you are using Windows 95 you must have the *MS Dial Up Networking 1.3 update* (**msdun13.exe**) installed. Additionally, users of early versions of Windows 95 (pre-OSR2) must install the *Winsock 2.0 update* (**w95w2setup.exe**). If you are using Windows NT, you must be logged in as *administrator* to run Setup Wizard.

Configuring the SnapGear VPN Router on your network

To configure the SnapGear VPN Router on your network:

1. Apply power to the SnapGear VPN Router. When the SnapGear VPN Router is powered on and it has no IP address, it will flash all front panel LEDs (except *POWER*). These LEDs will remain flashing until it has acquired an IP address.

2. Insert the *SnapGear VPN Router Installation CD* into the CD drive of any Windows PC on your network that meets the system requirements. From the **Start** menu, select **Run** and type **z:\setup** (where *z* is the letter of your CD drive).

3. Select the directory and Start menu group in which to install the software utilities for your SnapGear VPN Router.

4. The wizard will then search the network for your device. Once the wizard has located your device, you will be asked to enter an IP address (see Static Networks).

5. If you already have a DHCP server on the network (Dynamic Network), the SnapGear VPN Router will have automatically been assigned an IP address and its LEDs will no longer be flashing. Setup Wizard will locate the SnapGear VPN Router on the network.

Static Networks

Setup Wizard will ask you to enter an IP address for your SnapGear VPN Router. Select an unused IP address that you want to assign to the SnapGear VPN Router (e.g. *10.0.0.199*). The first three fields are auto-completed, based on the IP address and net mask of the local machine. Ensure that the SnapGear VPN Router is powered on and plugged into the network, then click **OK.** Setup Wizard will check that the IP address is available; if so, it will be assigned to the SnapGear VPN Router, otherwise you will be asked to try another.

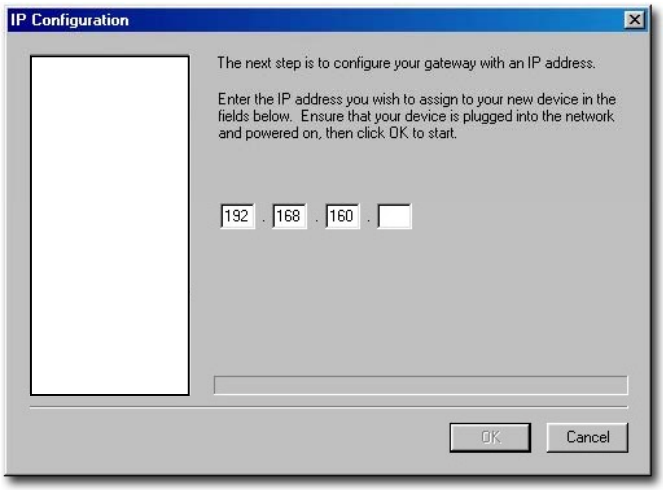

IP Configuration
The next step is to configure your gateway with an IP address.
Enter the IP address you wish to assign to your new device in the fields below. Ensure that your device is plugged into the network and powered on, then click OK to start.
192 . 168 . 160 .
OK
Cancel

Figure 2.1 Setup Wizard IP Setup

The LEDs on the front panel of the SnapGear VPN Router will remain flashing until the SnapGear VPN Router has been assigned an address. Once an IP address has been successfully assigned, they will all stop flashing.

If more than one SnapGear VPN Router device is found on the network, Setup Wizard will prompt you to select which one you want to set up based on the device's unique LAN port MAC address (see Figure 4). A MAC address is a unique physical address that all Ethernet adapters have assigned by manufacturers. A MAC address is fixed for the life of the hardware. This is a feature that makes a MAC address an excellent way of uniquely identifying equipment on a network, as you can be sure that no two will be the same. Your SnapGear VPN Router's LAN port MAC address is displayed on the underside of the device's case.

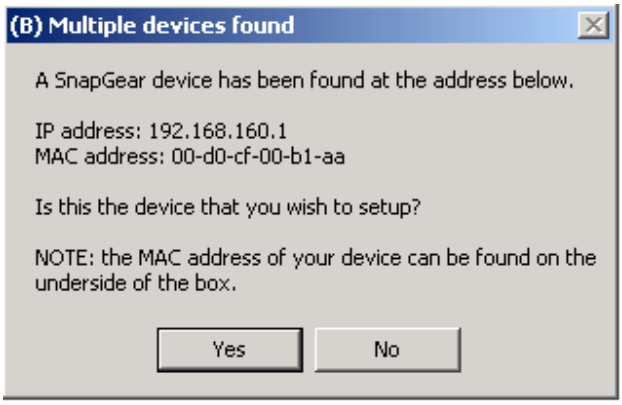

(B) Multiple devices found
A SnapGear device has been found at the address below.
IP address: 192.168.160.1
MAC address: 00-d0-cf-00-b1-aa
Is this the device that you wish to setup?
NOTE: the MAC address of your device can be found on the underside of the box.
Yes
No

Figure 2.2 Setup Wizard Internet setup

Once an IP address is allocated, the SnapGear Setup Wizard will then prompt you to change the SnapGear VPN Router's internal password. This password controls access to the *SnapGear VPN Router Configuration web pages* and the SnapGear VPN Router unit itself. It is recommended that the new password be chosen so that it is easy or you to remember but hard for others to guess. Your password must be kept secret to maintain the security provided by the SnapGear VPN Router.

When setup is complete, the wizard will prompt you to launch a web browser and open the SnapGear VPN Router Configuration web pages.

The SnapGear VPN Router Configuration web pages

Your SnapGear VPN Router is now configured – more configuration options are available through the *SnapGear VPN Router Configuration web pages*. To access these, select **SnapGear VPN Router Config Pages** from the *SnapGear VPN Router* Start Menu group, or, alternatively, point your web browser at the SnapGear VPN Router's IP address (e.g. *http://10.0.0.199/*). If you cannot access the web pages, it could be because your browser's proxy settings are not properly configured. In MSIE, this can be modified in *Tools*, *Internet Options*, *Connection* tab, *LAN settings*.

Initial setup using Linux

SnapGear VPN Router as shipped is configured with no Internet (IP) address.

When the SnapGear VPN Router is powered on and it has no IP address, it will flash all of its front panel LEDs (except the 'Power' LED). As soon as it acquires an address, it will stop flashing the LEDs.

The first setup task is to get an IP address into the SnapGear VPN Router. The primary mechanism for this is through DHCP or BOOTP. You may choose to use an existing local DHCP/BOOTP server, set up a new local DHCP/BOOTP server, or use the ***lin_set_ip*** program included on the SnapGear CD in the **/tools/** directory.

Using *lin_set_ip*

This program is a command line tool for assigning the SnapGear VPN Router an IP address. Depending on your system configuration, you may need to run this program with root privileges. You may also need to add an extra static route with:

route add –host 255.255.255.255 eth0

Where *eth0* is the name of your LAN interface (you may need to prefix this line with the *route* command's directory path, e.g. */sbin/route add*.. etc.).

Simply run *lin_set_ip* from the command line and enter the IP address you wish to assign to your SnapGear VPN Router. After a short time, the SnapGear VPN Router should be assigned the IP address and its LEDs will stop flashing.

Using an existing local DHCP or BOOTP server

If your local network is configured with a DHCP server then the SnapGear VPN Router will automatically acquire an address when it is attached to the network. You may need to consult your local DHCP server logs to find what address was assigned to the SnapGear VPN Router.

If you are unable to access your local DHCP server logs, you can find which address was assigned to your SnapGear VPN Router by issuing the following commands from a command prompt. These commands will work on both Windows and Linux operating systems.

1. ping <subnet broadcast address>

2. arp –a

Examine the output of the 'arp' command and locate the MAC address of your SnapGear VPN Router and the corresponding Internet Address. You can find the MAC address printed on the underside of your SnapGear VPN Router.

If your network has a BOOTP server then you can use this to set up the SnapGear VPN Router. Edit the BOOTP server's file, /etc/bootptab, and enter an entry for the SnapGear VPN Router. Use the Ethernet MAC address printed on a label on the bottom of the SnapGear VPN Router. Restart bootpd if it is running and connect the SnapGear VPN Router to the local network.

The SnapGear VPN Router will accept gateway and DNS server tags from DHCP or BOOTP, and set up the SnapGear VPN Router's routing tables appropriately.

Configuring a new local DHCP or BOOTP server

If your network currently has no DHCP or BOOTP server then you may choose to temporarily configure a local Linux system to be a bootp server. To do this:

1. Edit the /etc/inetd.conf file.
   - Search for the bootpd line. Most distributions ship with this disabled (that is, commented out with a "#" in front). Remove the "#" from the start of this line.
   - Save and exit the file.
2. Edit /etc/bootptab file:
   - Add a new line at the bottom that reads:

SnapGear VPN Router:ht=ethernet:ha=00d0cf000101:ip=192.168.0.1

- You will need to modify the IP address (tag "ip") to match your local network's addressing. Use an address in your local subnet. You will also need to modify the MAC address (tag "ha") to match that of your SnapGear VPN Router hardware. It should be printed on a label on the bottom of the SnapGear VPN Router box. You can optionally include gateway ("gw") and DNS ("ds" and "dn") tags as appropriate. See the manual page for *bootptab* if you are unsure.

- Save and exit the file.

3. Restart TCP/IP on your system. If you don't know how, then just reboot the Linux system. Once the system is running it should serve the IP address to the SnapGear VPN Router when it is connected to your network.

SnapGear Quick Setup Wizard

Once the initial network setup has been completed, all common configuration tasks can be carried out through the web pages.

The SnapGear Quick Setup Wizard is provided to guide you through the basic steps to configure the SnapGear VPN Router's LAN port and to connect to the Internet. To start the wizard, click on the **Quick Setup Wizard** link in the middle of the **SnapGear Management Console** configuration page. Modifying the configuration will require entering the SnapGear VPN Router's administrator password. The *username* field will be ignored, as there is no username. The factory default password is *default*.

LAN Port Quick Setup

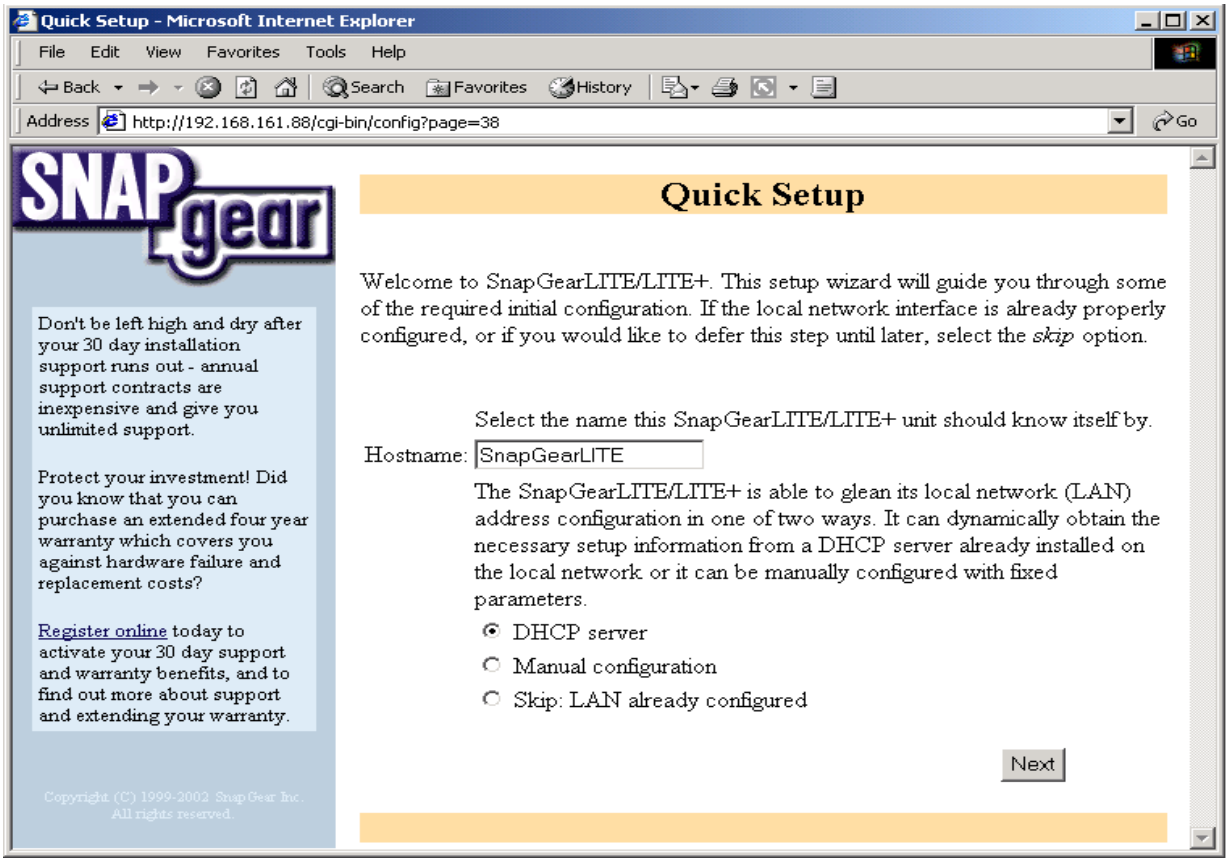

Quick Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.161.88/cgi-bin/config?page=38
Go
SNAPgear
Don't be left high and dry after your 30 day installation support runs out - annual support contracts are inexpensive and give you unlimited support.
Protect your investment! Did you know that you can purchase an extended four year warranty which covers you against hardware failure and replacement costs?
Register online today to activate your 30 day support and warranty benefits, and to find out more about support and extending your warranty.
Copyright (C) 1999-2002 SnapGear Inc.
All rights reserved.
Quick Setup
Welcome to SnapGearLITE/LITE+. This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the skip option.
Select the name this SnapGearLITE/LITE+ unit should know itself by.
Hostname: SnapGearLITE
The SnapGearLITE/LITE+ is able to glean its local network (LAN) address configuration in one of two ways. It can dynamically obtain the necessary setup information from a DHCP server already installed on the local network or it can be manually configured with fixed parameters.
DHCP server
Manual configuration
Skip: LAN already configured
Next

Figure 2.3 LAN Port Quick Setup

1. Enter the name by which the SnapGear VPN Router will be known on the LAN.

2. Choose the method used to set the LAN port network address configuration, either DHCP or manual.

3. If you choose **DHCP** or **Skip**, the **Next** button will take you to the **ISP Connection** configuration page.

4. If you choose **Manual,** the **Next** button takes you to the **Manual LAN Configuration** page where you must enter an **IP address** and a **Subnet mask** for the SnapGear LAN port.

ISP Connection Quick Setup

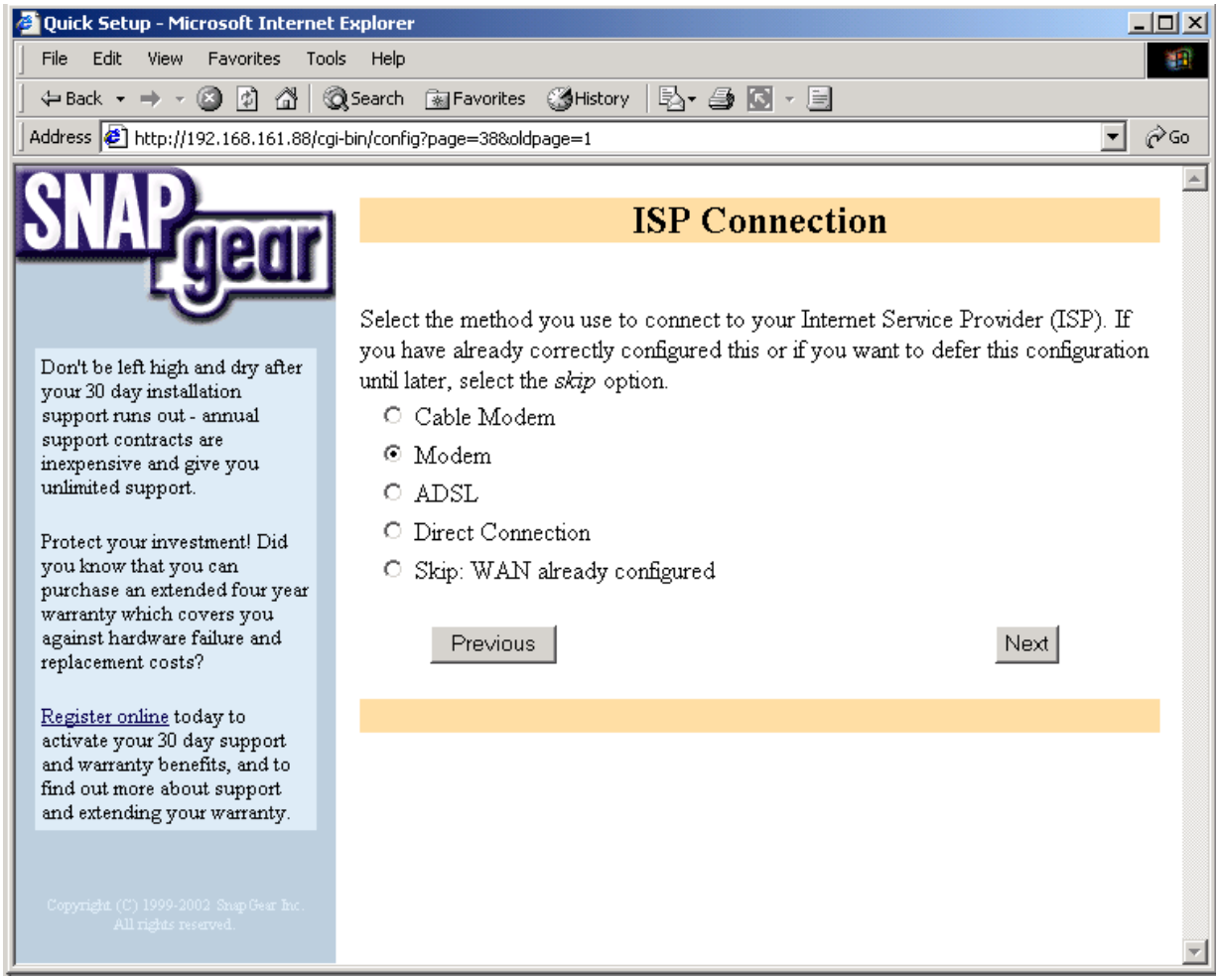

Quick Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.161.88/cgi-bin/config?page=38&oldpage=1
Go
SNAPgear
ISP Connection
Select the method you use to connect to your Internet Service Provider (ISP). If you have already correctly configured this or if you want to defer this configuration until later, select the skip option.
Cable Modem
Modem
ADSL
Direct Connection
Skip: WAN already configured
Previous
Next
Don't be left high and dry after your 30 day installation support runs out - annual support contracts are inexpensive and give you unlimited support.
Protect your investment! Did you know that you can purchase an extended four year warranty which covers you against hardware failure and replacement costs?
Register online today to activate your 30 day support and warranty benefits, and to find out more about support and extending your warranty.
Copyright (C) 1999-2002 SnapGear Inc.
All rights reserved.

Figure 2.4 ISP Connection Quick Setup

1. Select **Cable Modem, Modem, ADSL, or Direct** as the method you use to connect to your ISP. Note that **Direct connections** are those where the SnapGear Internet Port is connected to a LAN that has another gateway to the Internet.

2. For Cable Modems, you will be asked to specify your Cable Modem Service Provider. In most cases **Generic Cable Modem Provider** is the correct response.

3. If you connect to your ISP via a modem, you must also specify:

a. The serial port that is connected to your modem. The SnapGearSOHO+ and SnapGearPRO have two serial ports whereas the SnapGearLITE and SnapGearLITE+ have only one.

b. The name of your ISP.

c. The phone number used to dial your ISP.

d. The username and password for your ISP account.

4. If you connect to your ISP with ADSL (Asymmetric Digital Subscriber Line) the next step is to specify your ADSL connection type, either:

    a. Allow your SnapGear VPN Router to automatically detect your ADSL connection type. This is the best choice in most cases.

    b. **Use PPPoE to connect.** Choose this option if your ADSL modem communicates via PPPoE. PPPoE is the option to select if your ISP requires username and password authentication to access the Internet. You will also be asked to specify:

        i. The username and password for your ADSL connection.

        ii. If you want to **connect on demand** or stay connected continuously.

        iii. For **connect on demand** connections, the **idle disconnect time** (in minutes) is required.

    c. **Use DHCP to connect.** DHCP is used if your ISP did not provide you with a public IP address and/or instructed you to obtain an IP address automatically from a DHCP Server over the Internet.

    d. **Manually assign settings.** Choose this option if your ISP has provided a fixed IP address and a subnet mask and, optionally, a gateway address and a DNS address to be configured into the computer that connects to the ADSL modem.

5. For a **Direct Connection** you must configure the Internet port to either obtain its address information via DHCP or manually enter static values for **IP Address, Subnet Mask, Gateway Address,** and **DNS Address.** The **Gateway Address** is the address of the host to which all Internet network traffic is initially directed for further routing. The **DNS Address** is the address of the host that translates Internet domain names into IP addresses.

Configuring the PCs on your network

In order to access the Internet, all PCs on the network must have the IP address of the SnapGear VPN Router defined as their default gateway and be using the DNS server provided by the ISP. These details can either be manually (statically) entered, or dynamically assigned by a DHCP server each time the PCs boot.

To take advantage of the SnapGear VPN Router's DHCP server (or if you already have a DHCP server on the network), for each non-configured Windows workstation PC on the network, open the **Control Panel**, then **Network Control Panel** and select the **Obtain an IP address from a DHCP server** option, which is under **TCP/IP Properties** (see Figure 2.3).

Using Windows 95/98, this box can be located by clicking the **Configuration** pane, **TCP/IP-<your network adapter>**, **Properties**, then the **IP Address** pane.

Using Windows NT 4, this box can be located by clicking the **Protocols** pane, **TCP/IP**, **Properties**, then the **IP Address** pane.

Using Windows 2000, this box can be located by clicking **Start**, **Settings**, **Network and Dial-up Connections**, then right-clicking on **Local Area Connection**, click on **Properties**, select **Internet Protocol** then click **Properties**.

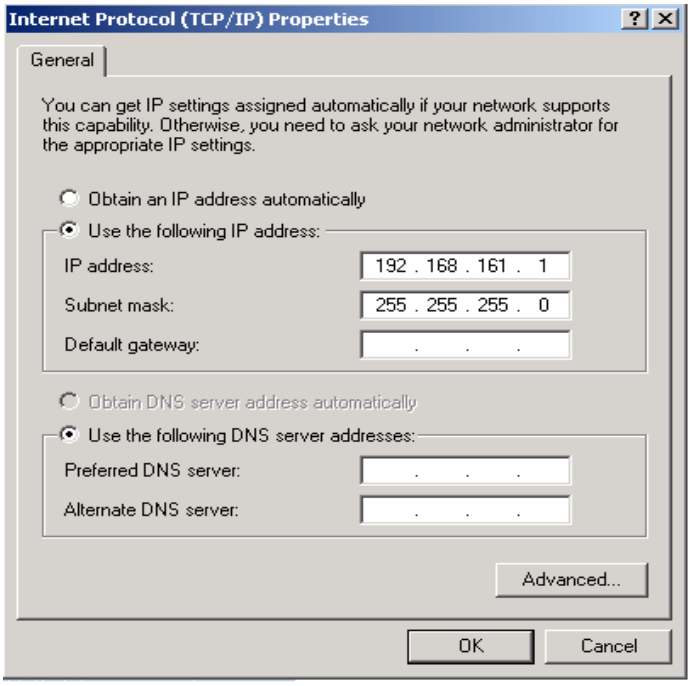

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 161 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2.3 Internet Protocol (TCP/IP) Properties

If you choose, you can manually configure the PCs on your network. For each non-configured Windows 2000 workstation PC on the network, open **TCP/IP Properties** (see above for details on the location of this option), and ensure that **Use the following IP address** is checked. Then add the following information:

- A unique IP address and appropriate subnet mask
- *Default Gateway* (enter the IP address of the SnapGear VPN Router)
- In the *DNS* tab, enter the DNS server address(es) provided by your ISP.

3. Connect to the Internet

This chapter will walk you through connecting the SnapGear VPN Router to your Internet Service Provider (ISP).

The SnapGear VPN Router provides secure Internet access through its robust embedded firewall. Its IP masquerading feature means that although users of your local network can see the outside world, the outside world can't see them, shielding your network from intruders. This simple, flexible solution also allows you to set packet filters (see *Chapter 6, Firewall*) to disallow any unwanted traffic into or out of your network.

The SnapGear VPN Router can connect to the Internet via an external dialup analog modem, ISDN modem, permanent analog modem, cable modem or DSL link (see Figure 6).

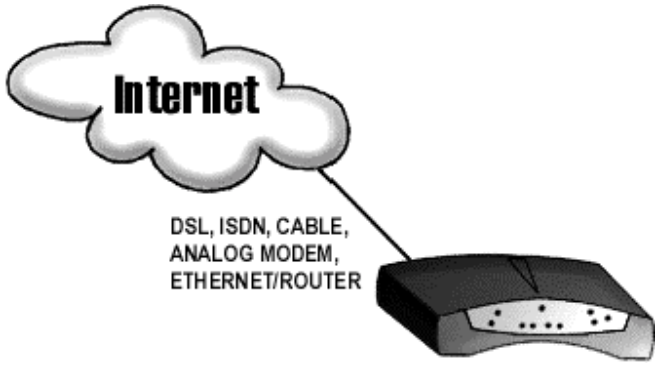


Figure 3.1 Internet connection

Physically connect modem device

To connect your office network to the Internet you must first physically attach your SnapGear VPN Router to a modem device (cable, ISDN, DSL or analog). For analog modems, attach the modem serial cable to one of the SnapGear VPN Router's serial ports (*COM1*, *COM2*). For digital connections (cable, ISDN, DSL), plug the cable into the *Internet* port.

***Warning**: ISDN connections – To connect to an ISDN line, the SnapGear VPN Router requires an intermediary device called a Terminal Adapter (TA). A Terminal Adapter will connect into your ISDN line and either have a serial or Ethernet interface that you can then connect to your SnapGear VPN Router.*

Select Internet connection

The next step is to select how you will be connecting your SnapGear VPN Router to the Internet. From the **SnapGear VPN Router Config Pages,** in the **Networking** menu, select **Connect to Internet** and choose the method you will use to connect to your local Internet Service Provider (ISP). You can connect to your ISP by any one of cable, ISDN, DSL or analog modem connections. Once the appropriate connection type has been selected, click **Continue**.

Connect to Internet – Cable Modem

With any SnapGear VPN Router, you can connect to the Internet using a cable modem. After selecting a cable connection, simply select your cable ISP from the list and click **Next**. If your provider does not appear here, select *Generic Cable Modem Provider.* For cable modem providers other than Generic, enter your username and password and click **Finish**. You are now ready to connect. Click the **Reboot** button to save your configuration and reboot your SnapGear VPN Router.

Connect to Internet – ADSL

To connect your SnapGear VPN Router to the Internet via ADSL, you must choose the connection method as **PPPoE, DHCP,** or **Manually Assign Settings.** Alternatively, the SnapGear VPN Router can determine the connection method automatically.

PPPoE is used if your ISP requires a username and a password authentication to access the Internet. DHCP is used if your ISP did not provide you with a public IP address and/or instructed you to obtain an IP automatically from a DHCP Server over the Internet. Manually assigning the settings on the SnapGearSOHO+'s Internet interface is required if your ISP has given you an IP address. Select the appropriate method and click **Apply.**

For PPPoE, you will be asked to enter the username and password for your ISP account. By default, your SnapGear VPN Router will maintain the ADSL connection continuously. However, you have the option of overriding the default to **Connect on Demand**. For on demand connections, you must also enter an **Idle Disconnect Time**, which is the time that the SnapGear VPN Router waits before disconnecting when the line is idle.

A hostname for your SnapGear VPN Router is required for DHCP connections.

Choose **Manually Assign Settings** and enter the **IP Address** and **Netmask** and optionally the **Gateway** and the **DNS Address** if your ISP has provided these. You will need to reboot the SnapGear VPN Router before the new configuration will take effect.

If you are unsure of the *ADSL Connection Method* to choose, select **Autodetect connection type**. Your SnapGear VPN Router will then attempt to automatically determine the appropriate connection method.

Connect to Internet – Direct

Choosing **Direct Connection** to the Internet will take you to the **IP Configuration** page. See *IP Configuration.*

Connect to Internet – Modem

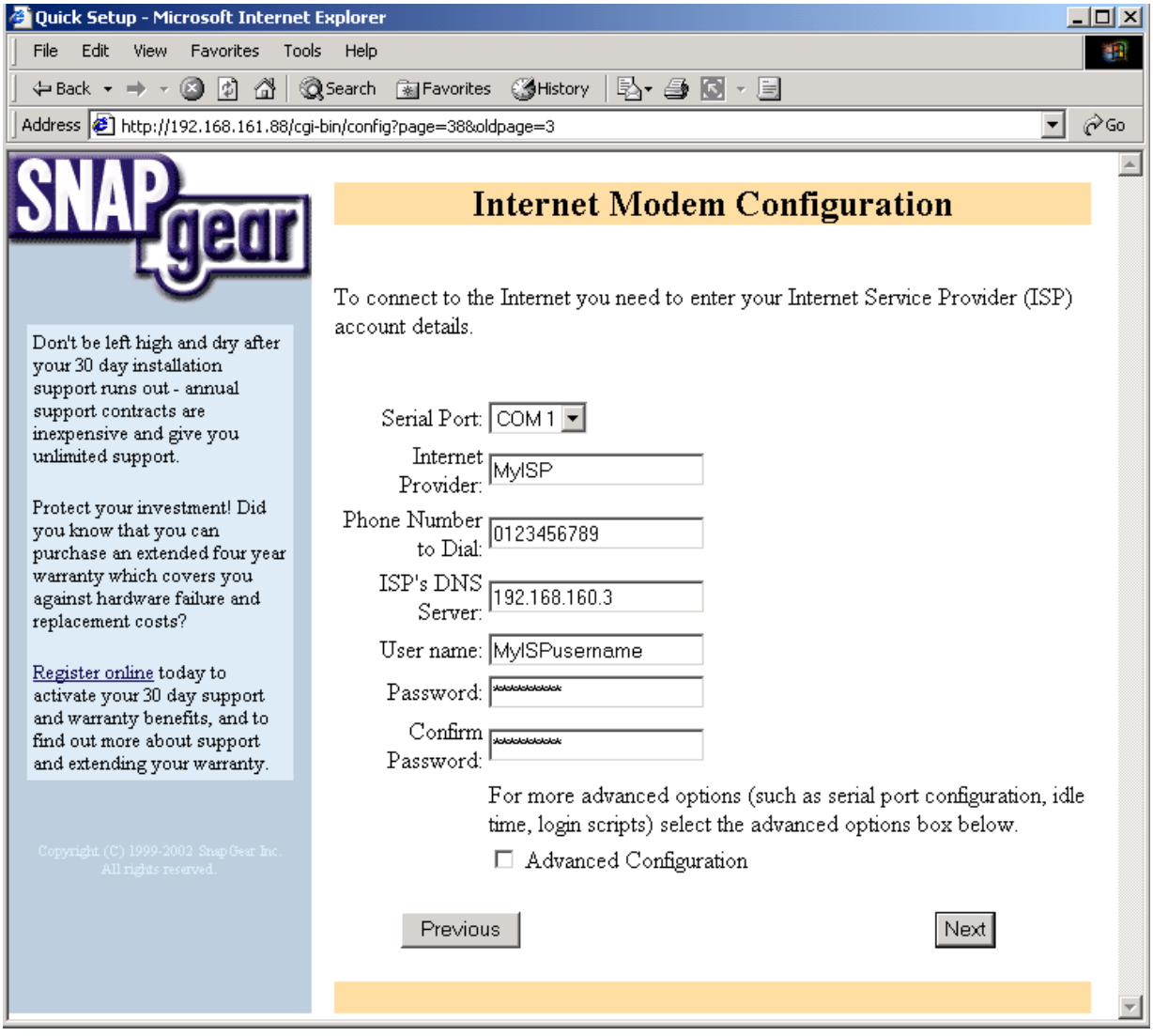

Quick Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.161.88/cgi-bin/config?page=38&oldpage=3
Go
SNAPgear
Don't be left high and dry after your 30 day installation support runs out - annual support contracts are inexpensive and give you unlimited support.
Protect your investment! Did you know that you can purchase an extended four year warranty which covers you against hardware failure and replacement costs?
Register online today to activate your 30 day support and warranty benefits, and to find out more about support and extending your warranty.
Copyright (C) 1999-2002 SnapGear Inc. All rights reserved.
Internet Modem Configuration
To connect to the Internet you need to enter your Internet Service Provider (ISP) account details.
Serial Port: COM 1
Internet Provider: MyISP
Phone Number to Dial: 0123456789
ISP's DNS Server: 192.168.160.3
User name: MyISPusername
Password:
Confirm Password:
For more advanced options (such as serial port configuration, idle time, login scripts) select the advanced options box below.
Advanced Configuration
Previous
Next

Figure 3.2 Setup modem Internet connection

If you selected a modem connection to the Internet you will be presented with the *Connect to Internet via a Modem* screen. The table below describes the fields and explains how to configure the dial up connection to your ISP.

Field	Description
SnapGear VPN Router port to dial out on	Select the SnapGear VPN Router COM (serial) port that you will use for the modem that will dial your ISP. This port will then be dedicated for the Internet connection. Any attempt to dial in on this COM port will be blocked. *Note: If a port was previously setup for dial-in and it is subsequently enabled for Internet access, then the dial-in function will be automatically disabled.*
Name of Internet provider	Enter the name of your Internet Service Provider (ISP).
Phone number to dial	Enter the number to dial to reach your Internet provider. If you are behind a PABX that requires you to dial a prefix such as 0 or 9 for an outside line, be sure to include the appropriate prefix.
ISP's DNS Server	Enter the DNS server address supplied by your ISP.
Username and password	Enter the unique username (login) given to you by your Internet provider and the corresponding password. Note that *Confirm Password* must match *Password*.
Idle timeout (This option is available in the Advanced Setup)	By default, the SnapGear VPN Router dials-on-demand (when there is traffic trying to reach the Internet) and disconnects if the connection is inactive (no traffic to or from the Internet) for 15 minutes. If using dial-on-demand, you can set this value to be anywhere in the range of 0 – 99 minutes. Selecting **Stay Connected** will disable the idle timeout.

Redial setup (This option is available in the Advanced Setup)	Should the dial up connection to the Internet fail, you can specify how many further dial attempts should be made before discontinuing in *Max Connection Attempts*, and how many seconds to wait between these redial attempts in *Time Between Redials*.
Statically assigned IP address (This option is available in the Advanced Setup)	The majority of Internet providers dynamically assign your connection an IP address when you dial in; however, some use statically pre-assigned addresses. If your ISP has given you a static IP address, enter it in *Local IP Address* and the address of the ISP gateway in *Remote IP Address*.

Configure PCs to use SnapGear VPN Router Internet gateway

The PCs on your network must be configured to use the SnapGear VPN Router as the default gateway for Internet access. See the section *Configuring the PCs on your network* (Chapter 2) for details on how this is done.

Establishing the connection

At this point, if you are using a modem or ISDN connection to your ISP, the SnapGear VPN Router will place a call automatically whenever an application requires access to the Internet (e.g. sending e-mail, browsing the web).

To establish the connection:

1. From any PC on the network, launch a browser application such as Internet Explorer or Netscape Navigator.
2. SnapGear VPN Router will dial the ISP and log in. On the front panel, you will see the relevant *COM* LED flash as the connection is established.
3. The *ONLINE* LED will light when the Internet link is set up and your browser will display the default Home page.
4. If *Dial-on-demand/Idle time* has been enabled, SnapGear VPN Router will also disconnect from the Internet when the connection has been idle for the specified period.

If you are using a permanent connection device, like a cable modem, then Internet access is automatic.

4. Dial-in server configuration

SnapGear VPN Router enables you to securely access your office network remotely. This chapter details how to set up the dial-in features. Note: Not all SnapGear VPN Router models support the RAS (Remote Access Server) functions found in this chapter.

The SnapGear VPN Router can be configured to receive dial-in calls from remote users or from remote sites. Remote users are individual users (for example telecommuters) who, directly from their client workstations, dial into modems connected to the SnapGear VPN Router's serial ports. Remote site dial-in connections can be LAN-to-LAN connections, where a router at a remote site establishes a dial-in link through a modem connected to the SnapGear VPN Router.

The SnapGear VPN Router dial-in facility establishes a PPP connection to the remote user or site. Dial-in requests are authenticated with usernames and passwords, which are verified by the SnapGear VPN Router.

Once authenticated, remote users and sites are connected and given the same access to the LAN resources as a local user.

To configure the SnapGear VPN Router for a dial-in connection:

1. Attach external modems to the relevant SnapGear VPN Router serial ports. Refer to Chapter 7, *Serial Ports and Modem Devices* for modem configuration details. Note that:

    - SnapGear VPN Router Models SOHO+ and PRO can support up to two dial-in connections.
    - SnapGear VPN Router Models LITE and LITE+ are unable to support dial-in connections.

2. Enable and configure the selected SnapGear VPN Router COM port for dial-in as detailed in *Dial-in Setup,* below.

3. Set up and configure user dial-in accounts for each person or site requiring dial-in access.

4. If required, packet filtering can be applied to dial-in connections, as detailed in Chapter 6, *Firewall.*

Dial-in setup

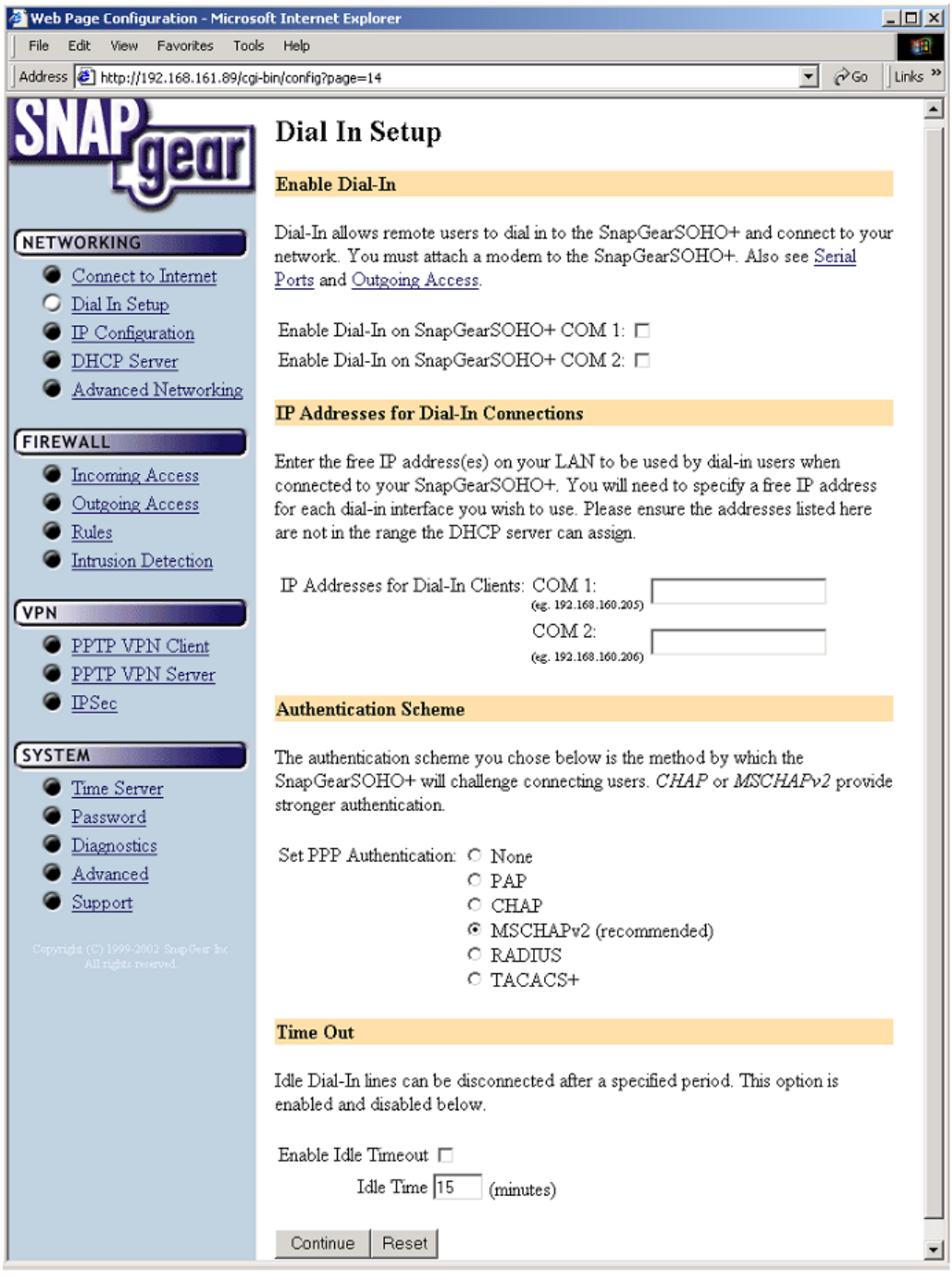

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.161.89/cgi-bin/config?page=14
Go
Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Dial In Setup
Enable Dial-In
Dial-In allows remote users to dial in to the SnapGearSOHO+ and connect to your network. You must attach a modem to the SnapGearSOHO+. Also see Serial Ports and Outgoing Access.
Enable Dial-In on SnapGearSOHO+ COM 1:
Enable Dial-In on SnapGearSOHO+ COM 2:
IP Addresses for Dial-In Connections
Enter the free IP address(es) on your LAN to be used by dial-in users when connected to your SnapGearSOHO+. You will need to specify a free IP address for each dial-in interface you wish to use. Please ensure the addresses listed here are not in the range the DHCP server can assign.
IP Addresses for Dial-In Clients: COM 1: (eg. 192.168.160.205)
COM 2: (eg. 192.168.160.206)
Authentication Scheme
The authentication scheme you chose below is the method by which the SnapGearSOHO+ will challenge connecting users. CHAP or MSCHAPv2 provide stronger authentication.
Set PPP Authentication:
None
PAP
CHAP
MSCHAPv2 (recommended)
RADIUS
TACACS+
Time Out
Idle Dial-In lines can be disconnected after a specified period. This option is enabled and disabled below.
Enable Idle Timeout
Idle Time 15 (minutes)
Continue
Reset

Figure 4.1 Dial-in setup

To enable and configure SnapGear VPN Router's Dial-In server, select **Dial-In Setup** from the **Networking** menu. The table below describes all the fields in the *Dial-In Setup* screen and explains how to enable and configure dial-in access on a SnapGear VPN Router COM port.

Field	Description
Enable Dial-in	To enable and configure dial-in, check the relevant COM port box. The selected port is now available for dial-in access. Otherwise, any attempt to dial in will be blocked. The current dial-in status of all the COM ports is displayed. If dial-in is already enabled, the check box will display a bold or shaded check mark. If not enabled, it will be clear. Note: A port that has been enabled for dial-in cannot be used simultaneously for dial-out activities, such as dial-on-demand Internet connection. If a port was previously set up for Internet access and is subsequently enabled for dial-in, the Internet access function will be disabled.
IP Addresses for Dial In users	To allow dial-in users access to the local network, they must be assigned local IP addresses. Specify a free IP address from your local network each dial-up client will use when connecting to the SnapGear VPN Router.
Authentication Scheme	The authentication scheme you choose is the method by which the SnapGear VPN Router will challenge users dialing into the network. Dial-in clients must be configured to use the selected authentication scheme. Select the desired option: *MSCHAPv2* is the most secure. *CHAP* is less secure, and similarly *PAP* is even less secure, but more common. If you choose None, no Username/Password authentication is performed on dial-in. *RADIUS* and *TACACS+* make use of a remote authentication server on the local network. When selected, you must enter the IP address of a server setup to use this scheme.
Idle Timeout	If a dial-in connection remains inactive, it can be automatically disconnected after a specified time period. Selecting **Enable idle timeout** will disconnect idle connections after 5 minutes. You can set this *Idle time* to be anywhere in the range of 0 – 99 minutes.

Once you have enabled and configured the selected SnapGear VPN Router COM ports to support dial-in, click **Continue** and you will be able to create and configure dial-in user accounts.

Dial-in user accounts

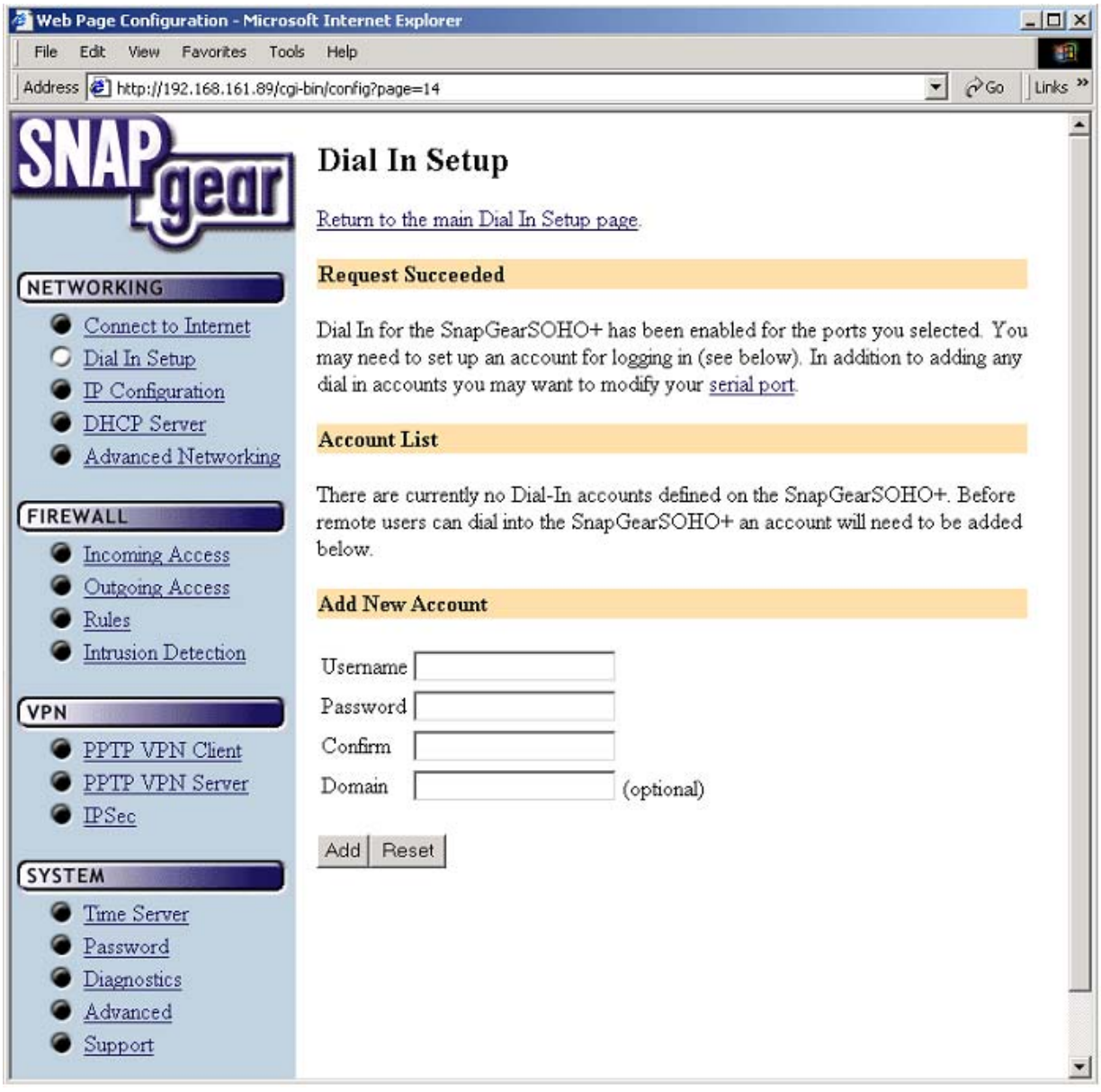


Figure 4.2 Dial-in user account creation

Before remote users can dial into the SnapGear VPN Router, you must set up user accounts. The field options in *Add New Account* are detailed in the table below:

Field	Description
Username	This username is required for dial-in authentication only. The name selected is case-sensitive (for example, *Jimsmith* is not the same as *jimsmith*).
Password	Enter the password for the remote dial-in user.
Confirm	Re-enter the password to confirm.
Domain	This field is optional and can be left blank. (If your network has a Windows NT server, you may wish to attach a domain name to your dial-in remote user accounts.)

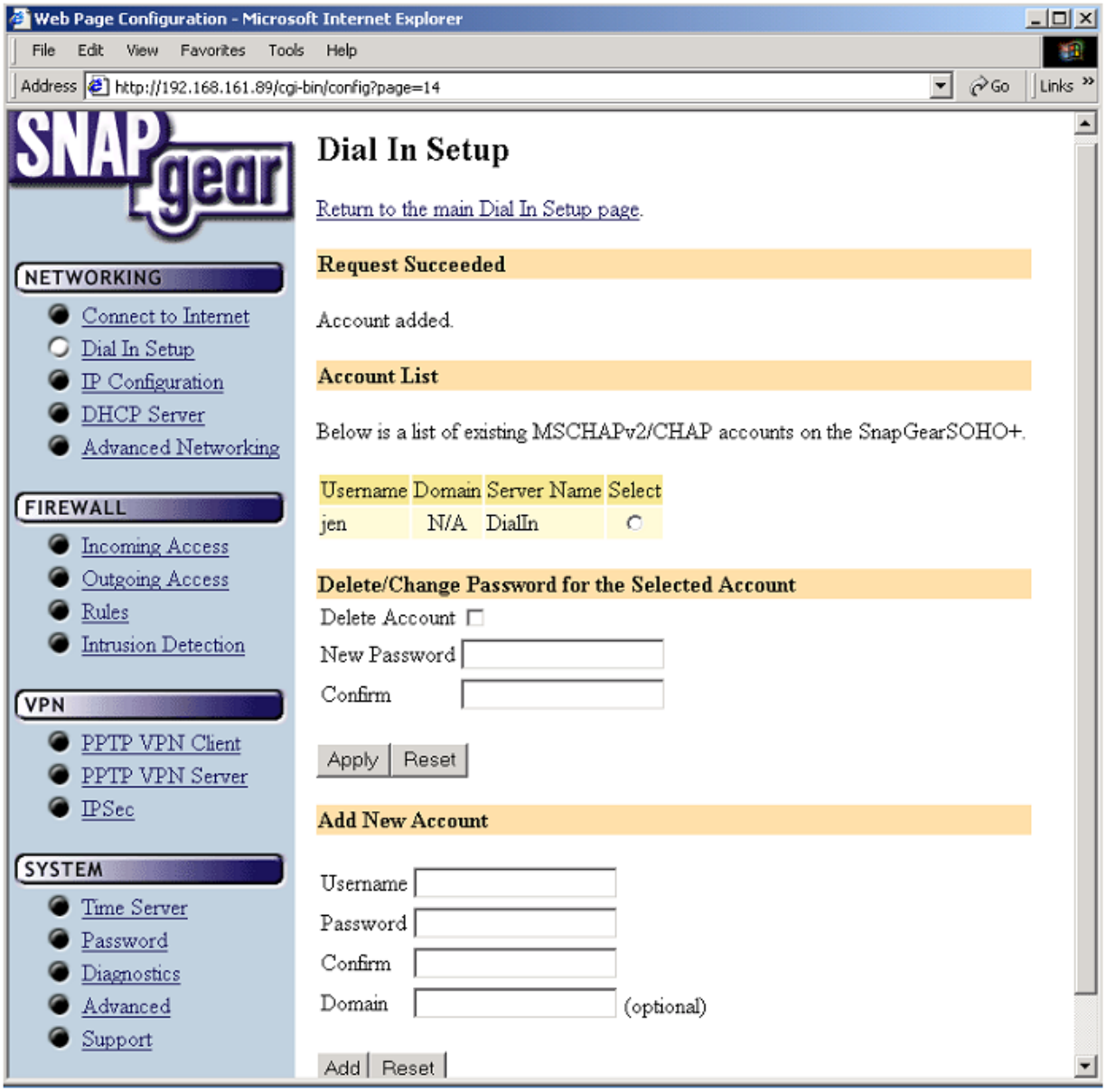


Figure 4.3 User Maintenance Screen

Account List

As new dial-in user accounts are added, they are displayed on the updated *Account List*.

To modify the password of an existing account, **Select** the account in the *Account List* then enter a new password identically in both the *New Password* and *Confirm* fields. Click **Apply** under the *Delete or Change Password for the Selected Account* heading, or reset if there is a mistake.

Similarly, to delete an existing account **Select** the account in the *Account List* then check **Delete** under the *Delete or Change Password for the Selected Account* heading.

If you request a change to a User Account and it is successful, the *Dial In Setup* screen will be represented with the change noted. If the change request is unsuccessful, an error will be reported as shown below.

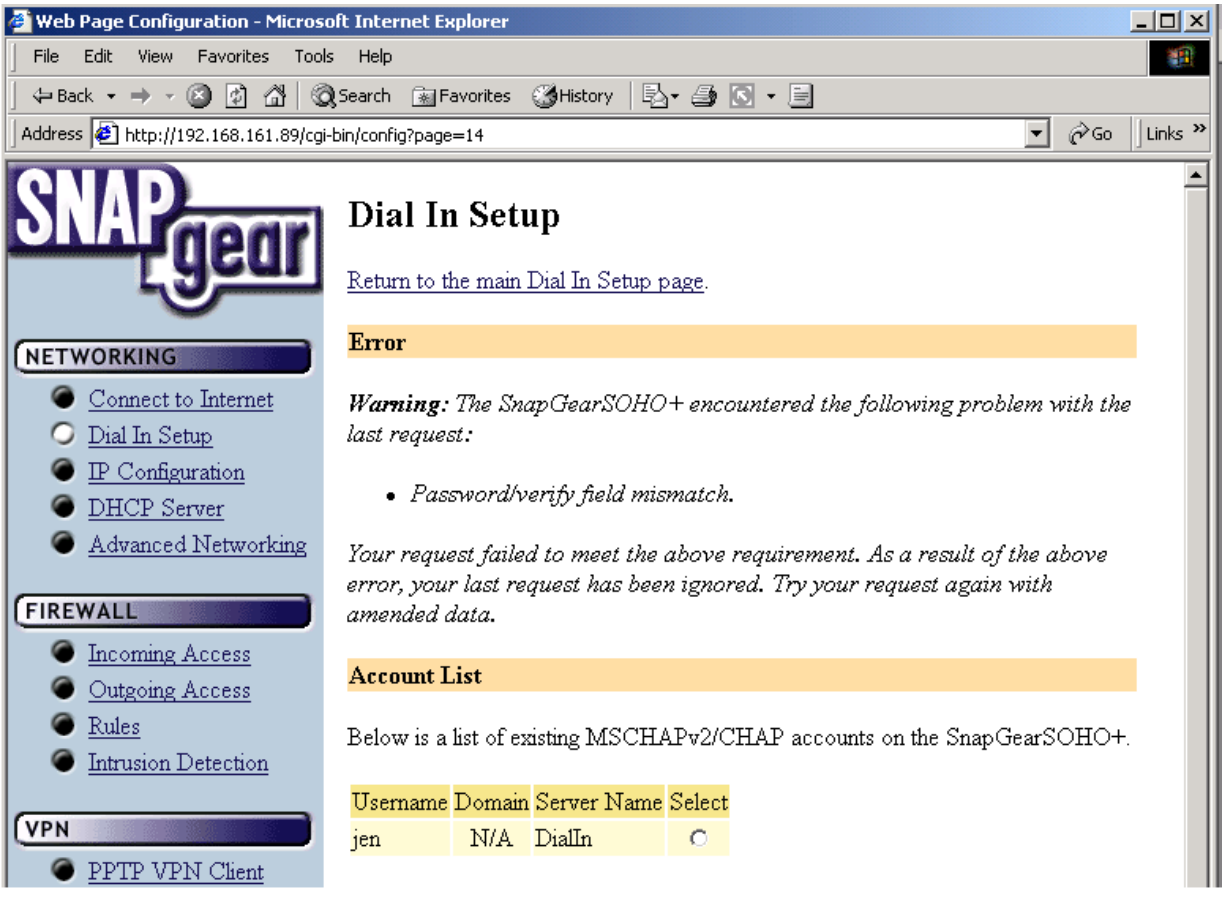

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.161.89/cgi-bin/config?page=14
Go Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
Dial In Setup
Return to the main Dial In Setup page.
Error
Warning: The SnapGearSOHO+ encountered the following problem with the last request:
Password/verify field mismatch.
Your request failed to meet the above requirement. As a result of the above error, your last request has been ignored. Try your request again with amended data.
Account List
Below is a list of existing MSCHAPv2/CHAP accounts on the SnapGearSOHO+.
Username Domain Server Name Select
jen N/A DialIn

Figure 4.4 Dial-in password error

You can continue to add more user accounts or modify account details. When complete, you can configure other SnapGear VPN Router functions simply by selecting the appropriate item from the *Network* or *System* menus.

One advanced SnapGear VPN Router function you may choose to configure now is to apply packet filtering to the dial-in service – as detailed in Chapter 6, *Firewall*.

Warning: *If you have enabled a SnapGear VPN Router COM port for dial-in, this port cannot be used simultaneously for dial-out activities such as dial-on-demand Internet connection. If a port was previously set up for Internet access, and is subsequently enabled for dial-in, the Internet access function will be automatically disabled.*

Remote user configuration

Remote users can dial-in connect through the SnapGear VPN Router using their standard Windows *Dial-Up Networking* software. A new dial-out connection must be set up on the remote PC, to dial the telephone number of the modem connected to the SnapGear VPN Router COM port.

Once dial-in connected, the user can access all network resources the same as a local user.

For Windows 95 and Windows 98:

From the *Dial-Up Networking* folder, double-click **Make New Connection**.

Type a *Connection Name* for your new dial-in connection.

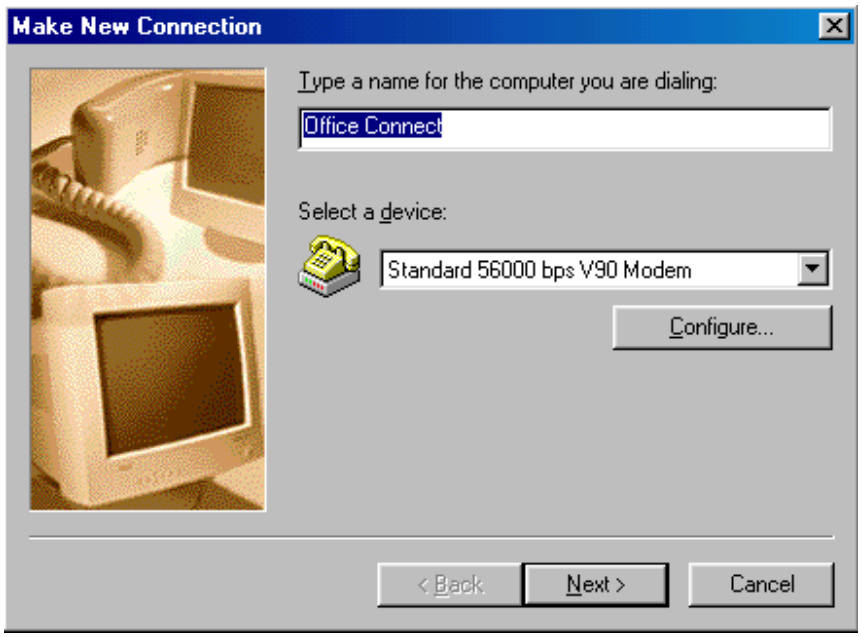


Figure 4.5 Make New Connection

From the *Select a device* pull down menu, select the modem you will be using.

Click **Next**, then fill in the details for the phone number of the modem connected to the SnapGear VPN Router.

Click **Finish**.

You should now see an icon in Dial-Up Networking named as your *Connection Name. C*lick on this once, then click on **File** and then **Properties**. Click on the **Server Types** tab on the top of the window.

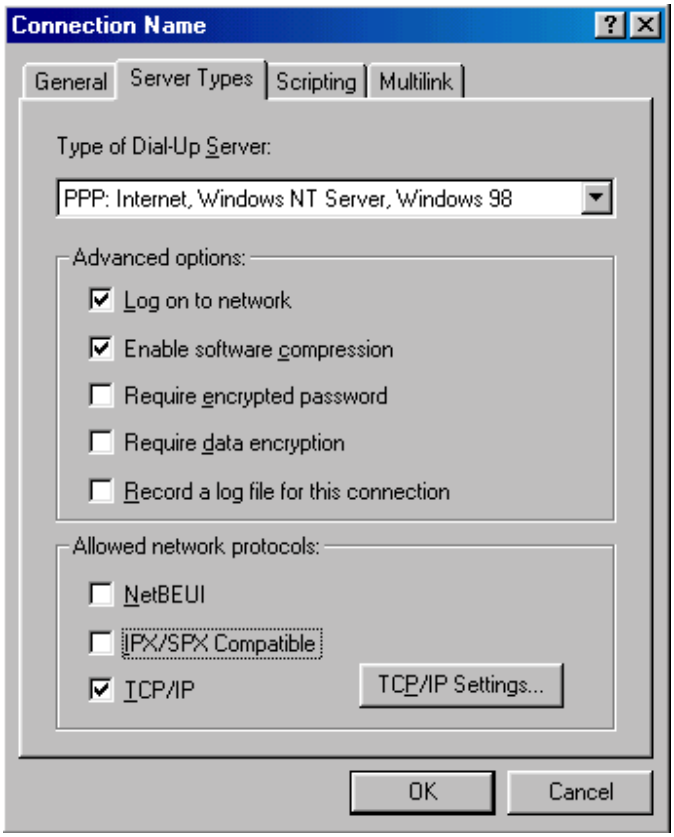


Figure 4.6 Connection Name

Check the **Log on to network** and **Enable software compression** check boxes. If you have set up your SnapGear VPN Router dial-in server to require *MSCHAP-2* authentication, you will also need to check the **Require encrypted password** check boxes. Leave the other *Advanced Options* unchecked.

Select the **TCP/IP** network protocols from the *Allowed network protocols* list. (*Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message will be returned.*)

Click **TCP/IP Settings**. Confirm that **Server Assigned IP Address**, **Server Assigned Name**, **Server Address, Use IP Header Compression** and **Use Default Gateway on Remote Network** are all checked. Click **OK**.

You can dial in and log on to the remote SnapGear VPN Router by double-clicking on your *Connection Name* icon. You will need to enter the **Username** and the **Password** that has been set up for the SnapGear VPN Router dial-in account, as indicated in the figure below.

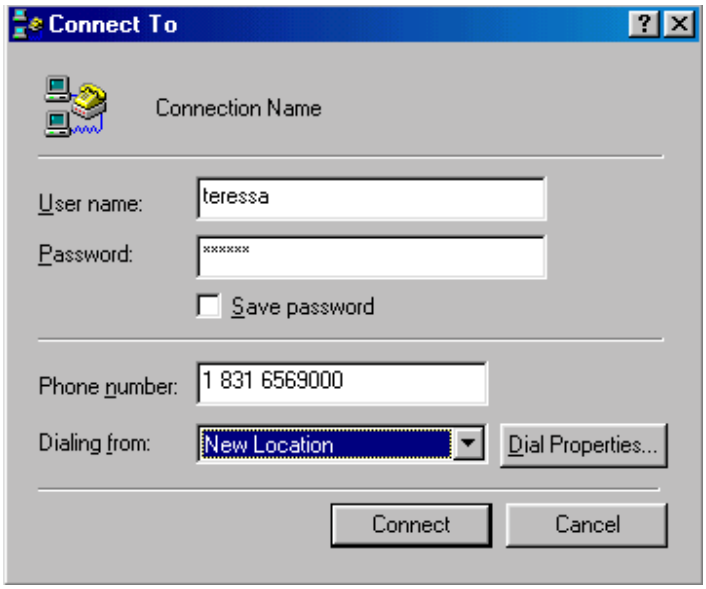


Figure 4.7 Connect To dialogue box

For Windows 2000:

To configure a remote access connection on a Windows 2000 computer, click **Start**, **Settings**, **Network and Dial-up Connections**. From the next window, choose **Make New Connection.**

The network connection wizard will guide you through setting up a remote access connection.

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel

Figure 4.8 Network Connection Wizard

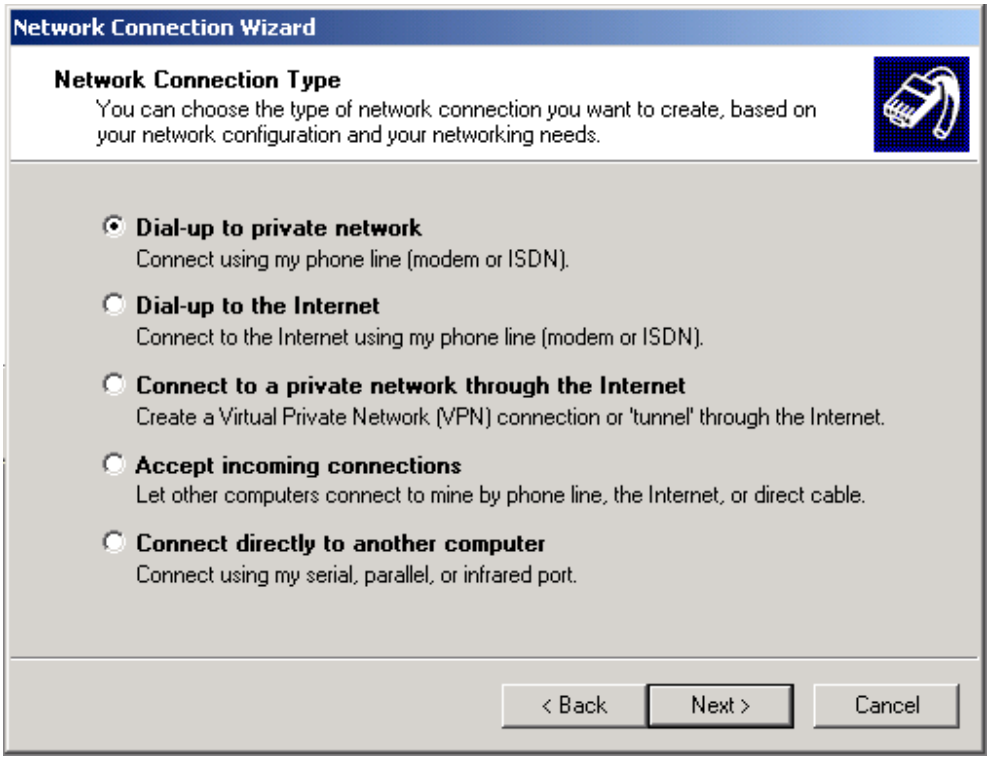

Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

Figure 4.9 Connection Type

Choose **Dial-up to private network** as the connection type.

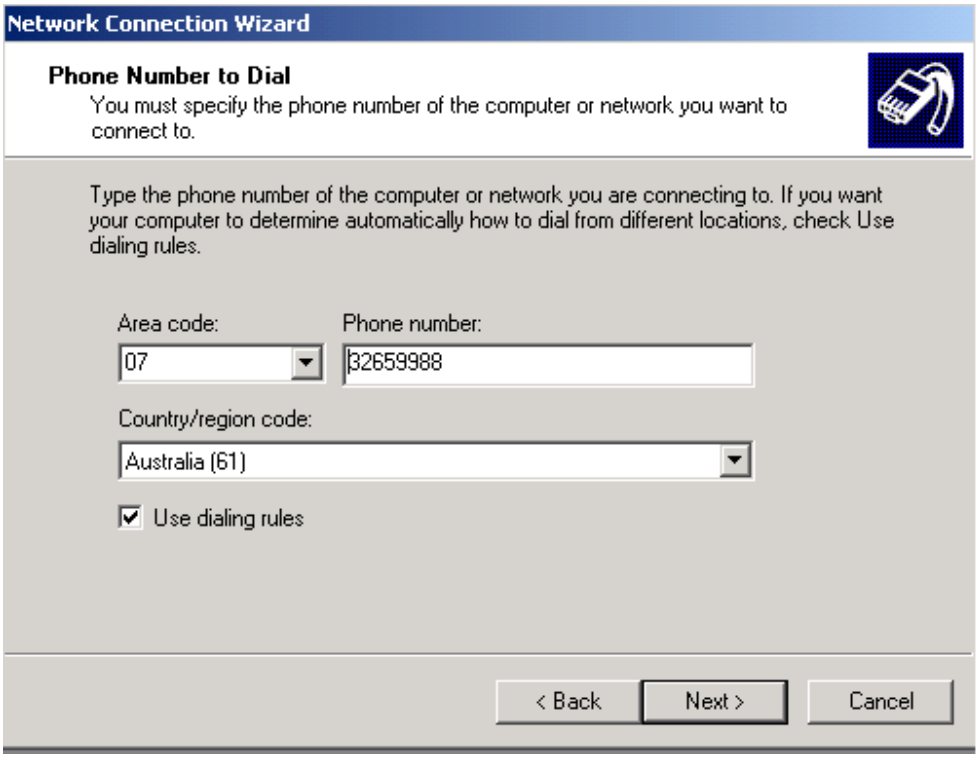

Network Connection Wizard
Phone Number to Dial
You must specify the phone number of the computer or network you want to connect to.
Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.
Area code:
Phone number:
07
32659988
Country/region code:
Australia (61)
Use dialing rules
< Back
Next >
Cancel

Figure 4.10 Phone number to dial

Tick **Use dialing rules** to enable you to choose a country code and area code. This feature is useful if you are using remote access in another state or overseas.

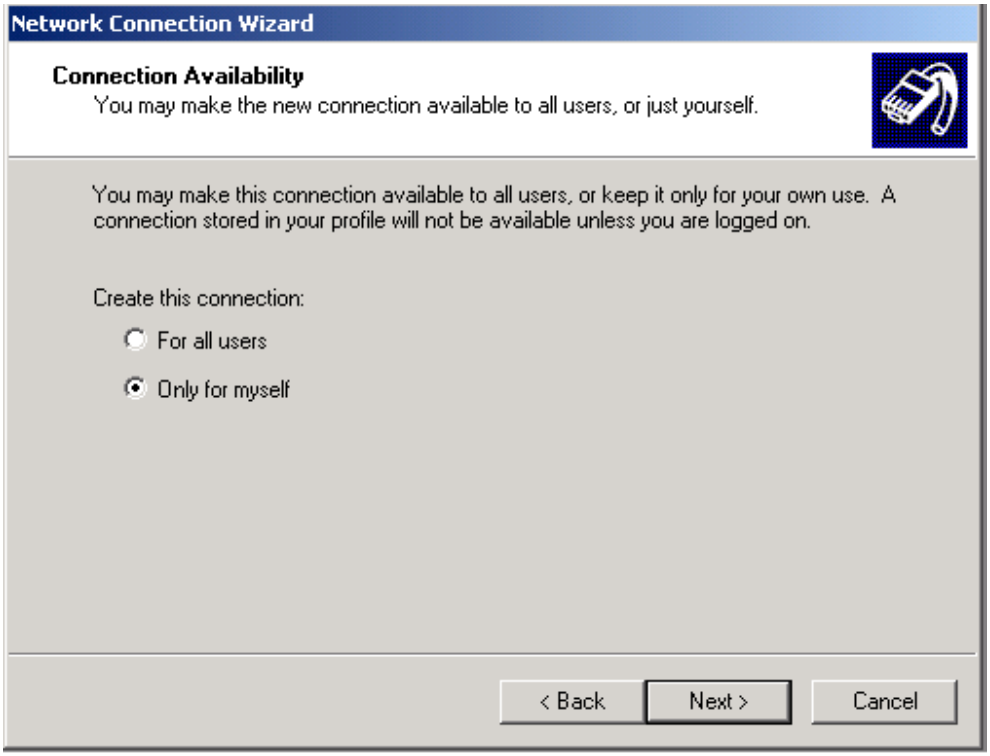

Network Connection Wizard
Connection Availability
You may make the new connection available to all users, or just yourself.
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.
Create this connection:
For all users
Only for myself
< Back
Next >
Cancel

Figure 4.11 Connection Availability

Select the option **Only for myself** to make the connection only available for you. This is a security feature that will not allow any other users who log onto your machine to use this remote access connection.

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Office Connect
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

Figure 4.12 Name of Connection

Enter a name for the connection and click **Finish** to complete the configuration. By ticking **Add a shortcut to my desktop,** an icon for the remote connection will appear on the desktop. To launch the new connection, double-click on the new icon on the desktop, and the remote access login screen will appear as in the next figure. If you did not create a desktop icon, click **Start, Settings, Network and Dial-up Connections** and choose the appropriate connection. You will need to enter the username and password that had been set up for the SnapGear VPN Router dial-in account.

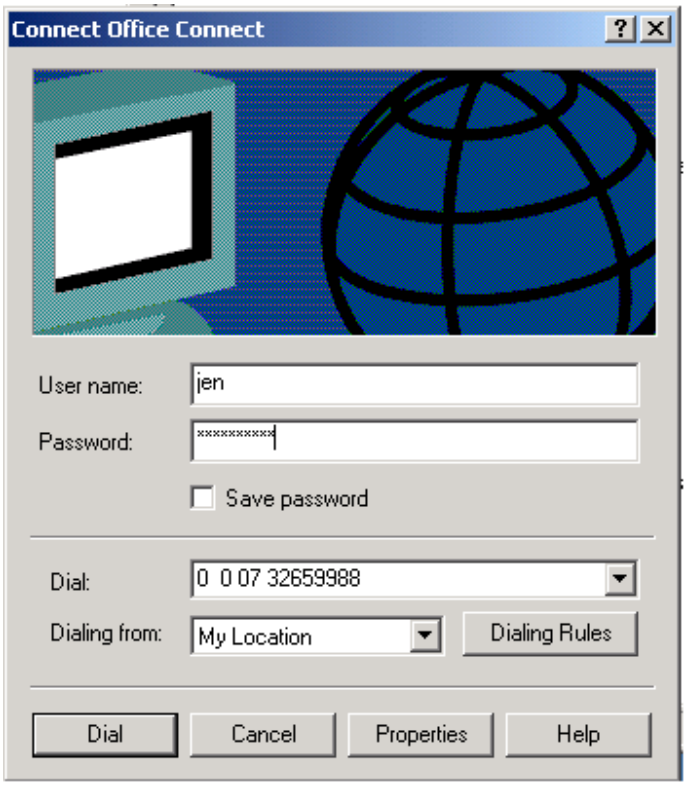


Figure 4.13 Remote Access Login Screen

5. Network Configuration

IP Configuration

Selecting **IP Configuration** from the *Networking* menu enables the user to set the IP address configuration of both the LAN and Internet interfaces.

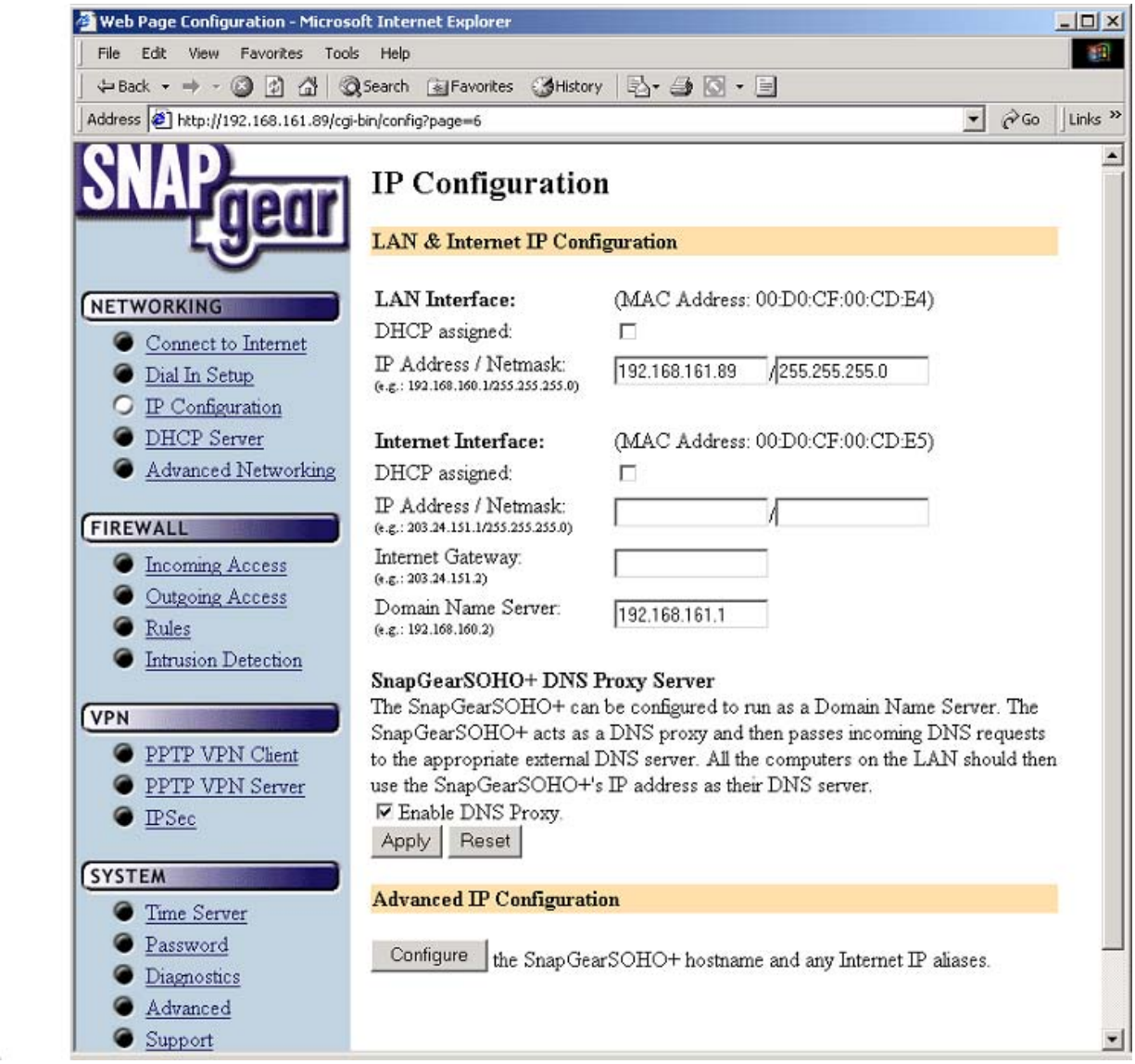


Figure 5.1 IP Configuration

To configure the LAN Interface of the SnapGear VPN router, simply choose between a dynamically or a statically assigned IP address. If the LAN interface of your SnapGear VPN Router obtains its IP address from a DHCP server on your local network, then check **DHCP assigned.** For a static IP address on the LAN interface, enter the **IP Address** and **Netmask** in the fields provided. Note that you must enter a static IP address if the SnapGear VPN router is to act as the DHCP server on your local network.

If your SnapGear VPN Router is configured for a **Direct Connection** to the Internet, you must also set the IP address for the Internet Interface. Check **DHCP assigned** if the IP address of the Internet Interface is set via a DHCP server, or enter the **IP Address** and **Netmask** if you have a static address for the Internet interface.

Enter the IP address of default gateway in the **Internet Gateway** field. The SnapGear VPN Router will send all packets not destined for the local network to this machine.

Enter the IP address of the DNS Server, which the SnapGear VPN Router will use to resolve domain names, into the **Domain Name Server** field. This should only be required if the SnapGear VPN Router is configured with a static IP address on the Internet interface and therefore doesn't receive its DNS server address automatically.

The SnapGear VPN Router can be configured to run as a Domain Name Server. The SnapGear VPN Router acts as a DNS proxy and passes incoming DNS requests to the appropriate external DNS server. If this is enabled, all the computers on the LAN should then specify the SnapGear VPN Router's IP address as their DNS server.

Advanced IP Configuration

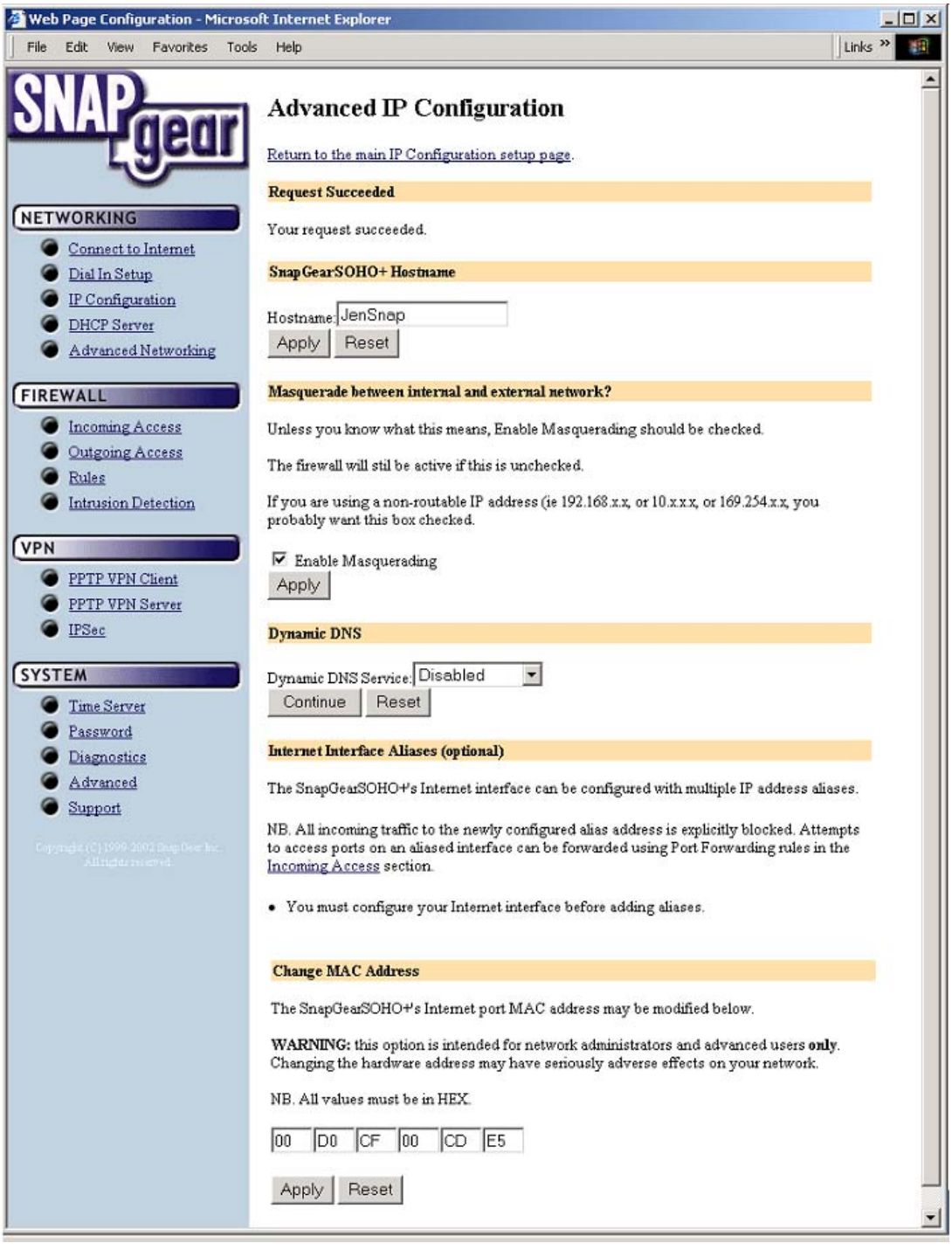

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Advanced IP Configuration
Return to the main IP Configuration setup page.
Request Succeeded
Your request succeeded.
SnapGearSOHO+ Hostname
Hostname: JenSnap
Apply Reset
Masquerade between internal and external network?
Unless you know what this means, Enable Masquerading should be checked.
The firewall will stil be active if this is unchecked.
If you are using a non-routable IP address (ie 192.168.x.x, or 10.x.x.x, or 169.254.x.x, you probably want this box checked.
Enable Masquerading
Apply
Dynamic DNS
Dynamic DNS Service: Disabled
Continue Reset
Internet Interface Aliases (optional)
The SnapGearSOHO+'s Internet interface can be configured with multiple IP address aliases.
NB. All incoming traffic to the newly configured alias address is explicitly blocked. Attempts to access ports on an aliased interface can be forwarded using Port Forwarding rules in the Incoming Access section.
You must configure your Internet interface before adding aliases.
Change MAC Address
The SnapGearSOHO+'s Internet port MAC address may be modified below.
WARNING: this option is intended for network administrators and advanced users only. Changing the hardware address may have seriously adverse effects on your network.
NB. All values must be in HEX.
00 D0 CF 00 CD E5
Apply Reset

Figure 5.2 Advanced IP Configuration

The **Hostname** is a descriptive name by which the SnapGear VPN Router will be known on the network.

The SnapGear VPN Router can utilize IP **Masquerading**, whereby users on the local network effectively share the one external IP address. Masquerading allows insiders to get out, without allowing outsiders in. By default, the Internet Interface is setup to Masquerade. Masquerading has the following advantages:

- Added security as only the address of the gateway is known by machines outside of your local network.
- All machines on your local network can access the Internet through a single ISP account.
- Only one public IP address is used and is shared by all machines on your local network, each of these local machines has its own private IP address.

SnapGear recommends leaving **Masquerade** set on the Internet Interface.

Internet Interface Aliases allows the SnapGear VPN Router to respond to multiple IP addresses on the Internet interface. You must also setup appropriate **Incoming Access** rules to allow traffic sent to the additional (aliased) IP addresses to be passed to the local network.

On rare occasions it may be necessary to change the Ethernet hardware or **MAC Address** of your SnapGear VPN router. Note that this is a globally unique address, which is specific to a single SnapGear VPN router. It is set by the manufacturer and should not normally be changed. However, you may need to change it if your ISP has configured your ADSL or cable modem to communicate only with a device that has a known MAC address.

DHCP Server

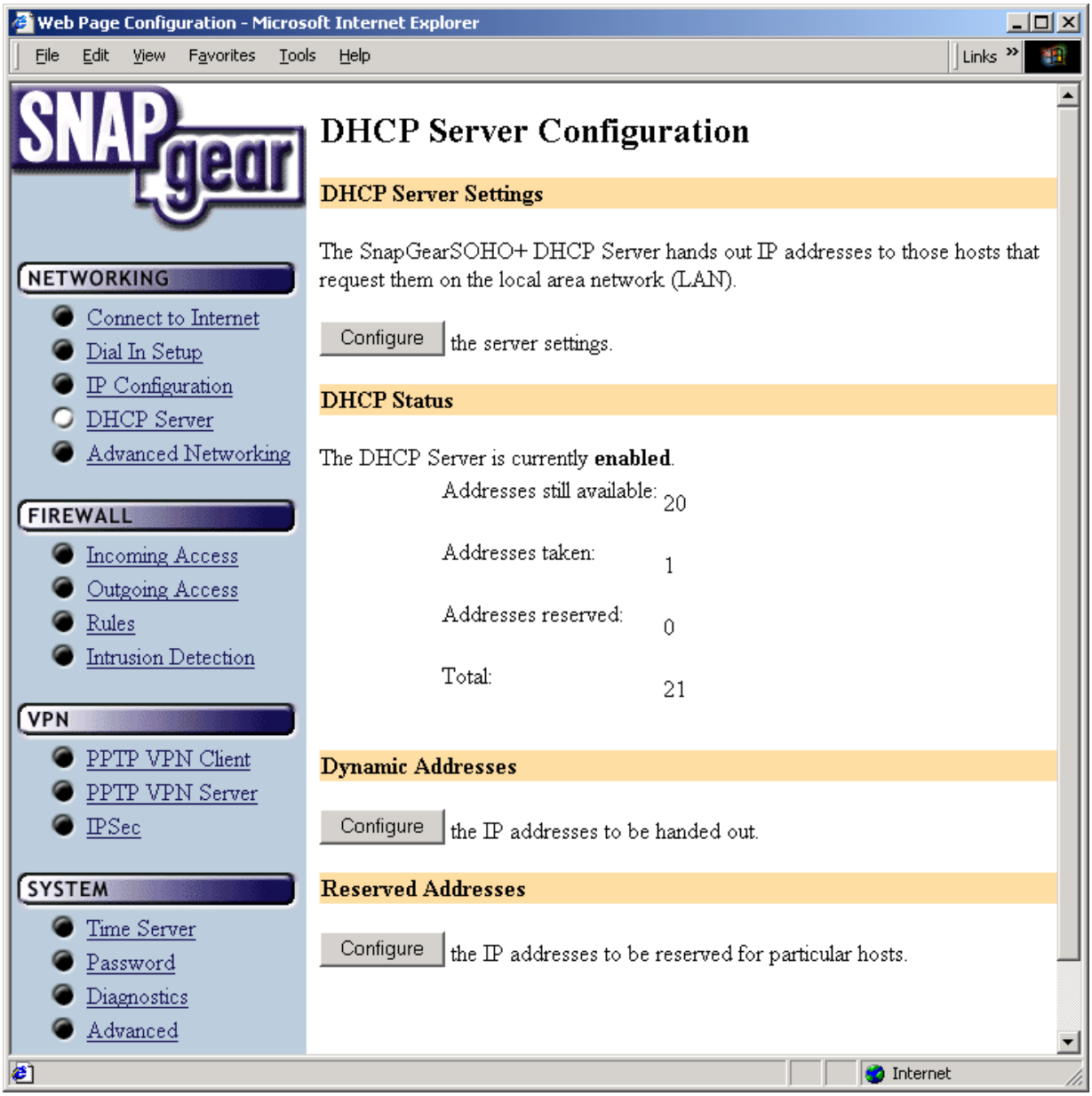


Figure 5.3 DHCP Server Configuration

To help keep your network design as simple as possible, your SnapGear VPN router can act as a DHCP server for machines on your local network. To configure your SnapGear VPN Router as a DHCP server, you must first set a static IP address and netmask on the LAN Interface (see *IP Configuration*).

Click **Configure the server settings** on the *DHCP Server Configuration* to:

- **Enable DHCP server** by checking the box. Conversely uncheck the box to disable the DHCP server.

- Enter the **Gateway Address** to be handed out to DHCP clients. Note that this will normally be the IP address of the SnapGear VPN Router's LAN Interface.

- Enter the **DNS Address** to be handed out to DHCP clients. This field can be left blank for automatic DNS server assignment. Note that if your SnapGear VPN Router is configured for DNS masquerading, then you should either leave this field blank or enter the IP address of the SnapGear VPN Router's LAN Interface.

- Enter IP address of the WINS server to be handed out to DHCP clients, in the **WINS Address** field.

- Enter the **Default Lease Time** and **Maximum Lease Time** in seconds. The lease time is the time for which a dynamically assigned IP will be valid.

Click **Configure the IP addresses to be handed out** to enter the addresses from which the DHCP server will allocate IP addresses to machines on the local network.

To reserve a particular IP address for a specific machine click on **Configure the IP addresses to be reserved for particular hosts.** For each reserved IP address, you must enter the **Hostname and MAC Address** of the machine as well as the **IP Address** that is to be allocated to this machine.

To take advantage of the SnapGear VPN Router's DHCP server functionality, you should configure the other machines on your local network to obtain their IP addresses dynamically from the SnapGear VPN Router. See the documentation that came with these machines for detailed instructions on how to configure their local network interfaces.

Advanced Networking

The *Advanced Networking* page allows users to perform the following diagnostic tasks:

- Perform a **Ping Test.**

- Perform a **Trace Route Test.**

- View the **Interface Configuration.**

- View the **Kernel Route Table.**

Access to the advanced networking configuration tasks of **Traffic Shaping** and **Additional Routes** is also via the *Advanced Networking* page.

Traffic Shaping

The **Traffic Shaping** feature of your SnapGear VPN Router allows you to allocate **High, Medium,** or **Low** priority to the following services: domain (tcp), domain (udp), ftp, ftp-data, http, https, imap, irc, nntp, ntp, pop3, smtp, ssh, and telnet. **Traffic Shaping** provides a level of control over the relative performance of various types of IP traffic. Note that this advanced feature is provided to allow expert users to fine tune their networks.

Additional Routes

Expert users may add additional static routes using this feature of the SnapGear VPN Router. These routes are in addition to those created automatically by the SnapGear VPN Router's configuration scripts.

6. Firewall

The SnapGear VPN Router comes with a full featured, stateful firewall. The firewall allows you to control both incoming and outgoing access and to detect intrusion attempts, so that PCs on the office network can be provided with tailored Internet access facilities and are shielded from malicious attacks. The SnapGear Firewall filters packets at the network layer, determines whether session packets are legitimate and evaluates contents of packets at the application layer thus providing maximum protection for your private network.

Incoming Access

Clicking **Incoming Access** on the *Firewall* menu will take you to the *Incoming Access* configuration page, where you can configure the firewall to control external access to services provided by the SnapGear VPN router itself as well as services provided by machines on your local network.

Incoming Access - Administration Services

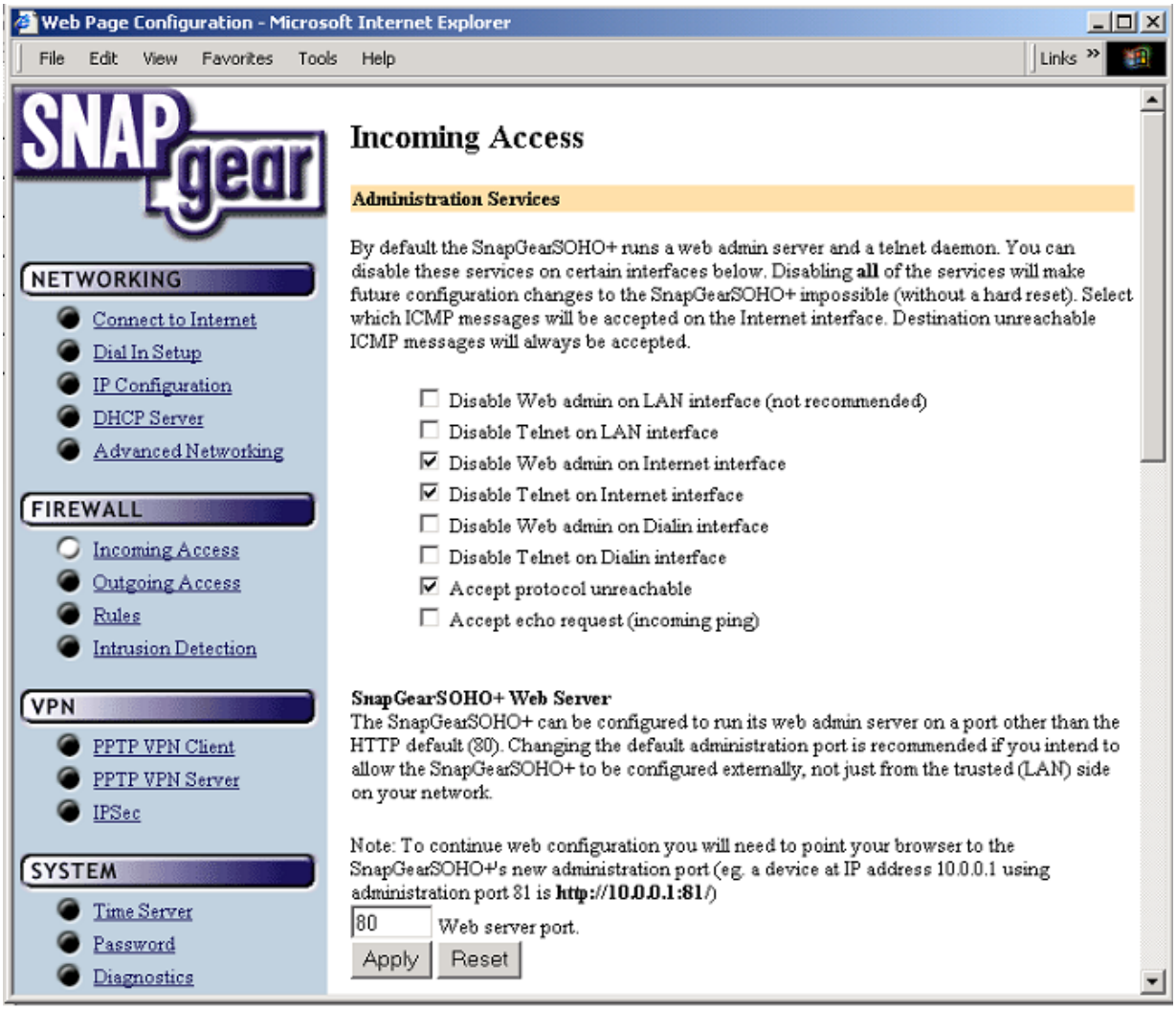

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Incoming Access
Administration Services
By default the SnapGearSOHO+ runs a web admin server and a telnet daemon. You can disable these services on certain interfaces below. Disabling all of the services will make future configuration changes to the SnapGearSOHO+ impossible (without a hard reset). Select which ICMP messages will be accepted on the Internet interface. Destination unreachable ICMP messages will always be accepted.
Disable Web admin on LAN interface (not recommended)
Disable Telnet on LAN interface
Disable Web admin on Internet interface
Disable Telnet on Internet interface
Disable Web admin on Dialin interface
Disable Telnet on Dialin interface
Accept protocol unreachable
Accept echo request (incoming ping)
SnapGearSOHO+ Web Server
The SnapGearSOHO+ can be configured to run its web admin server on a port other than the HTTP default (80). Changing the default administration port is recommended if you intend to allow the SnapGearSOHO+ to be configured externally, not just from the trusted (LAN) side on your network.
Note: To continue web configuration you will need to point your browser to the SnapGearSOHO+'s new administration port (eg. a device at IP address 10.0.0.1 using administration port 81 is http://10.0.0.1:81/)
80
Web server port.
Apply
Reset

Figure 6.1 Incoming Access configuration

By default the SnapGear VPN Router runs a web administration server and a telnet daemon. Access to these services can be restricted to specific interfaces. For example, you may want to restrict access to the SnapGear VPN Router's configuration web pages (**Web Admin)** to only machines on your local network. Note that it is inadvisable to disallow all services, as this will make future configuration changes impossible without resetting your SnapGear VPN Router to its factory default settings.

You can also select which ICMP messages will be accepted on the Internet interface. Destination unreachable ICMP messages will always be accepted. For example, disallowing echo requests will mean that your SnapGear VPN Router will not respond to pings on its Internet Interface.

The SnapGear VPN Router's web administration pages are usually accessed on the HTTP default port, that is, port 80. Changing this port number is advisable if you are allowing Internet access to web administration pages as this will hide your web administration pages from a casual web server who happens across your SnapGear VPN Router on the Internet. Note that after changing the web server port number, you must include the new port number in the URL to access the web administration pages. For example, if you change the web administration port number to 88, the URL to access the web administration will be similar to http://192.168.22.1:88.

External Access to Services

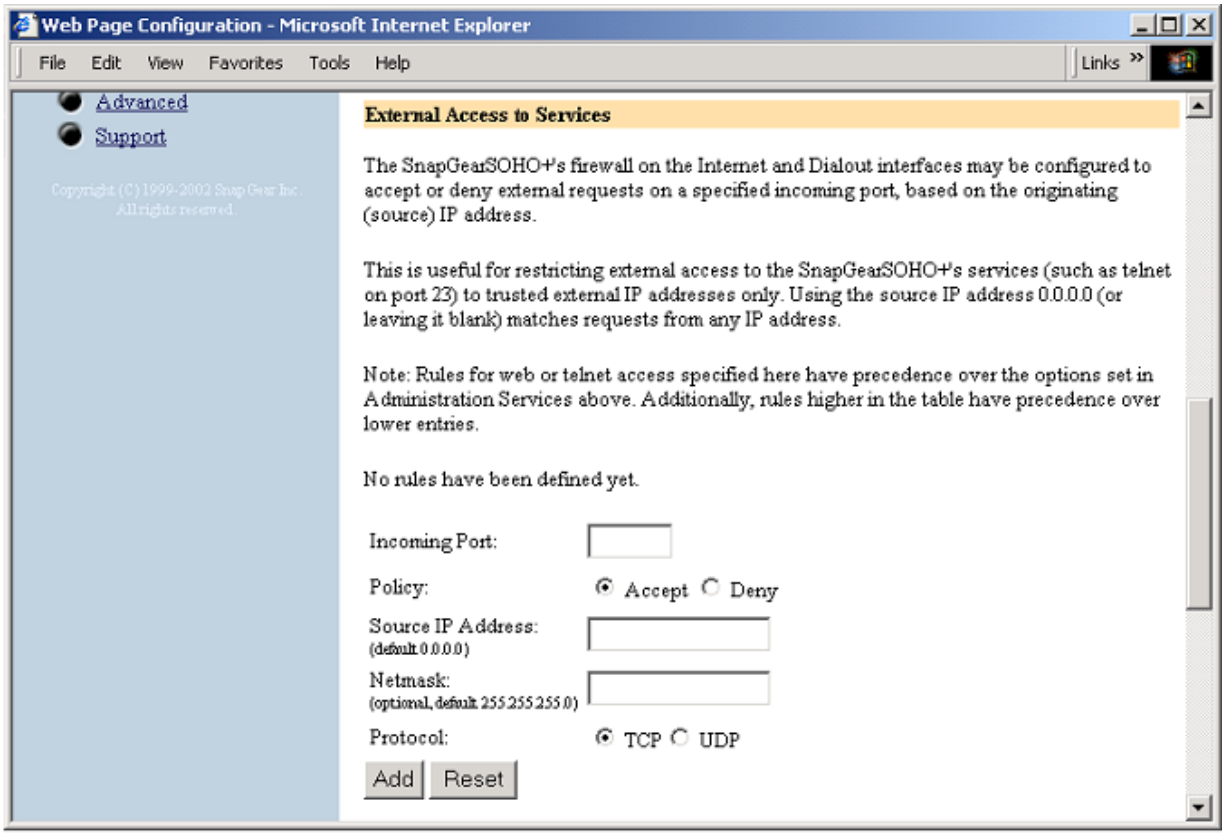

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Advanced
Support
External Access to Services
The SnapGearSOHO+'s firewall on the Internet and Dialout interfaces may be configured to accept or deny external requests on a specified incoming port, based on the originating (source) IP address.
This is useful for restricting external access to the SnapGearSOHO+'s services (such as telnet on port 23) to trusted external IP addresses only. Using the source IP address 0.0.0.0 (or leaving it blank) matches requests from any IP address.
Note: Rules for web or telnet access specified here have precedence over the options set in Administration Services above. Additionally, rules higher in the table have precedence over lower entries.
No rules have been defined yet.
Incoming Port:
Policy: Accept Deny
Source IP Address: (default 0.0.0.0)
Netmask: (optional, default 255.255.255.0)
Protocol: TCP UDP
Add Reset

Figure 6.2 Configure External Access to Services

The SnapGear VPN Router's firewall on the Internet interface can be configured to accept or deny external requests on a specified incoming port, based on the originating (source) IP address.

This is useful for restricting external access to the SnapGear VPN Router's services (such as telnet on port 23) to trusted external IP addresses only. Note that the options specified in the *Administration Services* section for disabling web or telnet access on the Internet interface have lower priority than any rules that you specify for web or telnet access here.

Port Forwarding

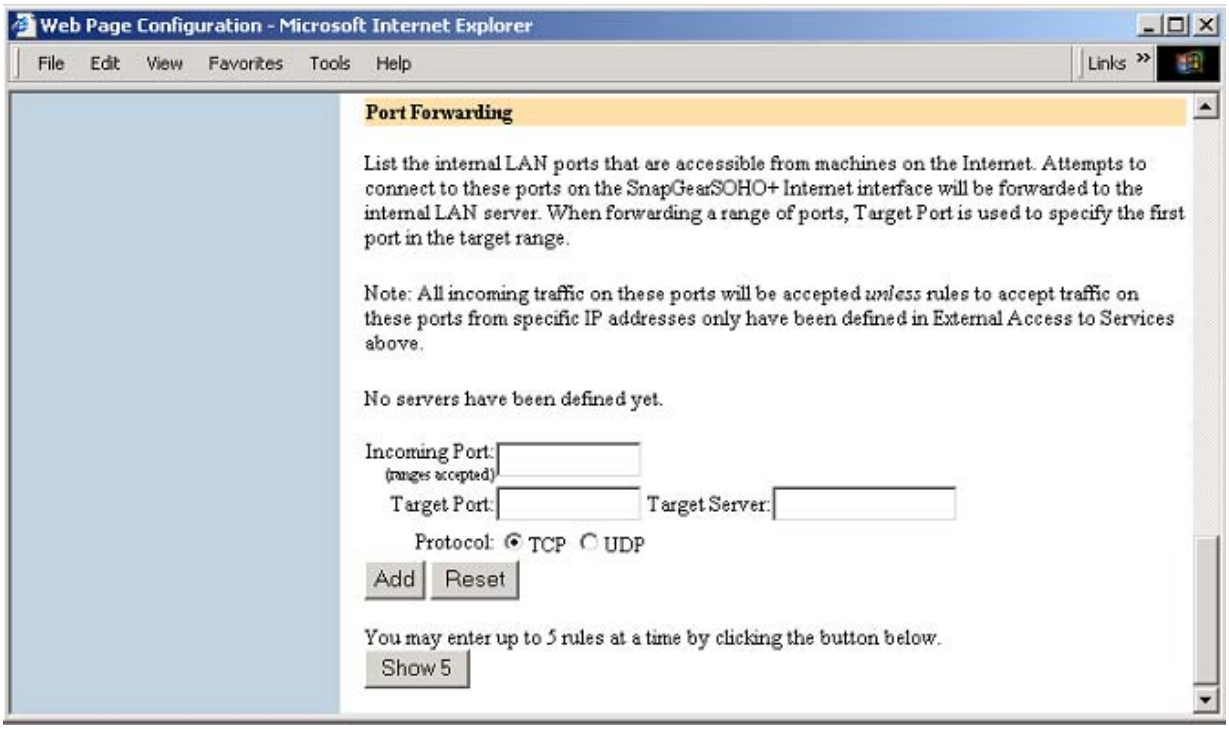

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Port Forwarding
List the internal LAN ports that are accessible from machines on the Internet. Attempts to connect to these ports on the SnapGearSOHO+ Internet interface will be forwarded to the internal LAN server. When forwarding a range of ports, Target Port is used to specify the first port in the target range.
Note: All incoming traffic on these ports will be accepted unless rules to accept traffic on these ports from specific IP addresses only have been defined in External Access to Services above.
No servers have been defined yet.
Incoming Port: (ranges accepted)
Target Port:
Target Server:
Protocol: TCP UDP
Add Reset
You may enter up to 5 rules at a time by clicking the button below.
Show 5

Figure 6.3 Port Forwarding Configuration

Port forwarding allows the SnapGear VPN Router to control access to services provided by machines on your private network from users on the Internet. Requests coming into the SnapGear VPN Router on the specified **Incoming Port(s)** will be forwarded to the **Target Port** on the **Target Server**.

Outgoing Access

Your SnapGear VPN router can be configured to restrict certain network traffic going out the Internet interface. These restrictions can either be applied to specific hosts or networks (defined by IP address), or globally across all hosts on your internal local area network (LAN). Outgoing Access restrictions are applied by denying a group of services (for example: web and email) from specific hosts or networks or globally across all hosts.

Your SnapGear VPN Router's Outgoing Access Restrictions are configured by using *security group classes*. Click on the **security group classes'** link on the *Outgoing Access Configuration* page to set the restrictions for each *security group class.* Each *security group class* can be configured to restrict certain TCP/IP application protocols or to block specified TCP and UDP ports.

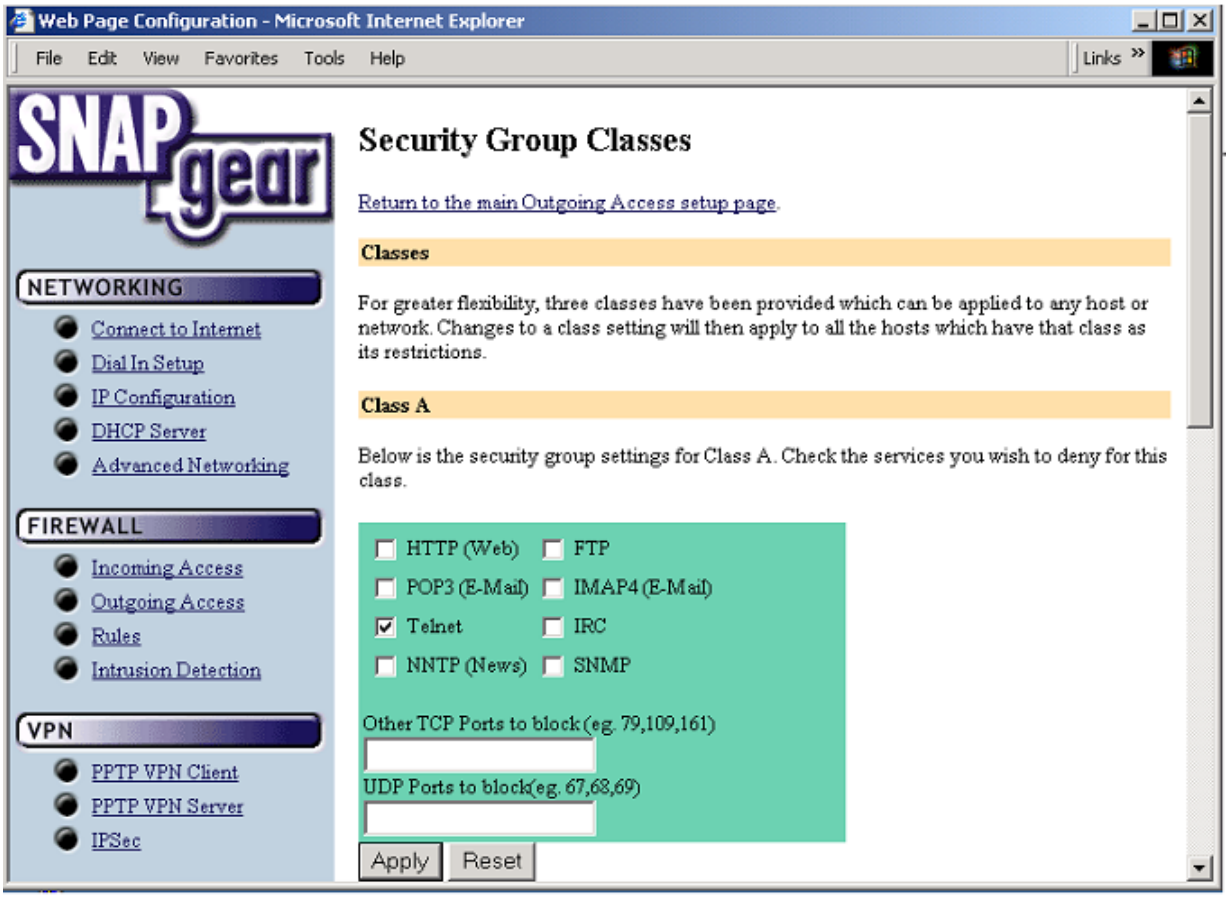


Figure 6.4 Security Group Classes Configuration

Once you have specified the restrictions you want each security group class to impose, you can apply these restrictions globally to all machines on your local network or to specific machines or networks. Use the *Add Hosts or Networks* section to specify the specific machines or networks from which you would like to restrict outgoing access.

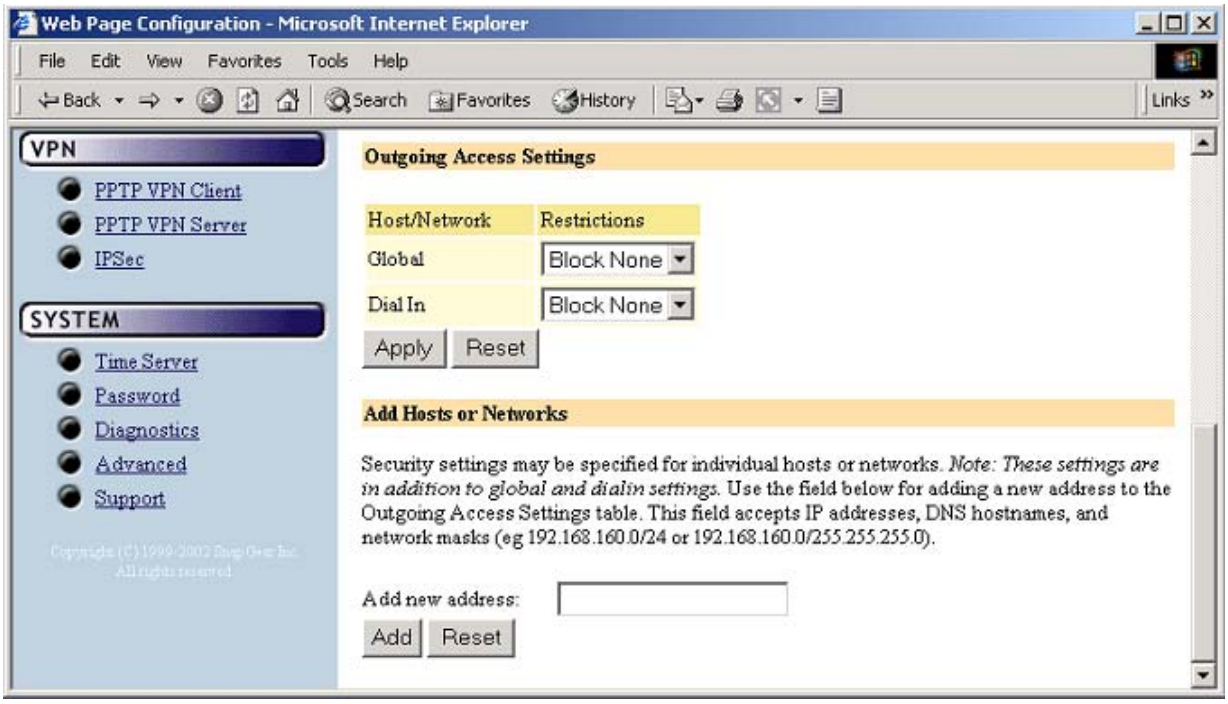


Figure 6.5 Outgoing Access Settings

Firewall Rules

The *Firewall Rules* configuration page allows firewall experts to view the current firewall rules and to add custom firewall rules. Access to this page is by clicking on **Rules** in the *Firewall* menu. Please note that only experts on Firewalls and *iptables* rules will have the ability to add effective custom firewall rules. Configuring the SnapGear Firewall via the *Incoming Access* and *Outgoing Access* configuration pages is adequate for all but some very specialized applications.

Intruder Detection and Blocking

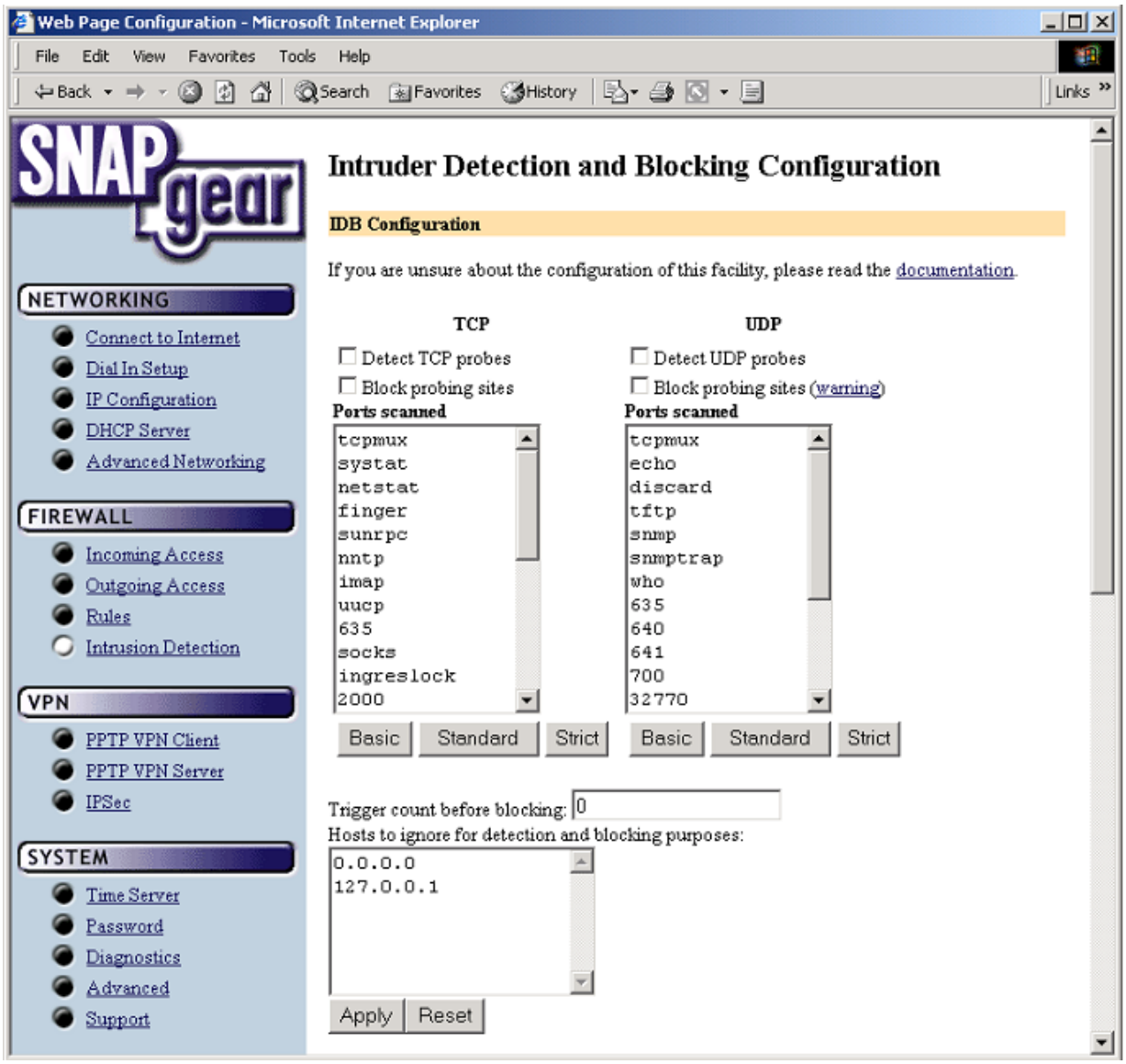


Figure 6.6 Intruder Detection and Blocking configuration

Intruder Detection and Blocking (IDB) operates by offering a number of services to the outside world, which are then monitored for connection attempts. Remote machines that attempt to connect to these services generate a system log entry providing details of the access attempt and then the access attempt is categorically denied. Since network scans are often a prelude to a concerted attempt to compromise a host, the ability to deny all access from hosts that have attempted to scan monitored ports is also available. Select one or both of the *block* options to enable this facility and such hosts will be automatically blocked once detected.

The list of network ports that can be monitored can be edited freely. In addition, several short cut buttons are available which provide pre-selected lists of services to monitor. The **basic** button installs a bare bones selection of ports to monitor whilst still providing sufficient coverage to detect many intruder scans. The **standard** option extends this coverage by introducing additional monitored ports so that most intruder scans will be detected early. The **strict** button installs a comprehensive selection of ports to monitor that should be sufficient to detect all but the stealthiest of scans.

The trigger count specifies the number of times a host is permitted to attempt to connect to monitored services before being blocked. This option only has an effect if one of the blocking options above is enabled. Generally, the value of the trigger count should be in the *0* to *2* range. A setting of *0* represents an immediate blocking of probing hosts. Larger settings mean more attempts are permitted before blocking and whilst allowing the attacker a little more latitude, such settings will reduce the number of false positives.

The ignore list contains a listing of host IP addresses which are to be ignored by IDB for detection and blocking purposes. This list may be free extended so that trusted servers and hosts will not be blocked. The two addresses *0.0.0.0* and *127.0.0.1* cannot be removed from the ignore list since they represent the IDB host.

Warning: *A word of caution about automatically blocking UDP requests. Because the source address of such requests can be forged by an attacker without much difficulty, a host that automatically blocks UDP probes can be tricked into restricting access from legitimate services. Proper firewall rules and ignored hosts lists will significantly reduce the risk of this happening.*

7. Virtual Private Networking

Virtual Private Networking enables two or more locations to communicate securely and effectively, usually across a public network such as the Internet. Three key traits of VPN technology are:

- Privacy (no one else can see what you are communicating)
- Authentication (you know who you are communicating with)
- Integrity (no one else can tamper with your messages/data)

With Virtual Private Networking, you can access the office network securely across the Internet using PPTP (Point-to-Point Tunneling Protocol) or IPSec. If you take your portable computer on a business trip, you can dial a local number to connect to your Internet access provider and then create a second connection, or tunnel, into your office network across the Internet. You will have the same access to your corporate network as if you were connected directly to it from your office. Similarly, telecommuters can set up a VPN tunnel over their cable modem or DSL links to their local Internet Service Providers.

With the SnapGear VPN Router you can establish a secure VPN over the Internet using either PPTP or IPSec. IPSec provides the better security, however, PPTP may be the VPN protocol to use when integrating with existing Microsoft infrastructure. The SnapGear VPN Router provides a PPTP server to enable remote Windows clients to securely access your office network. Using the SnapGear VPN Router's PPTP client or IPSec you can also connect your office network to one or more remote networks. This chapter explains how to configure the PPTP server and client, as well as IPSec in your SnapGear VPN Router, and how to set up remote clients to connect to your VPN tunnel.

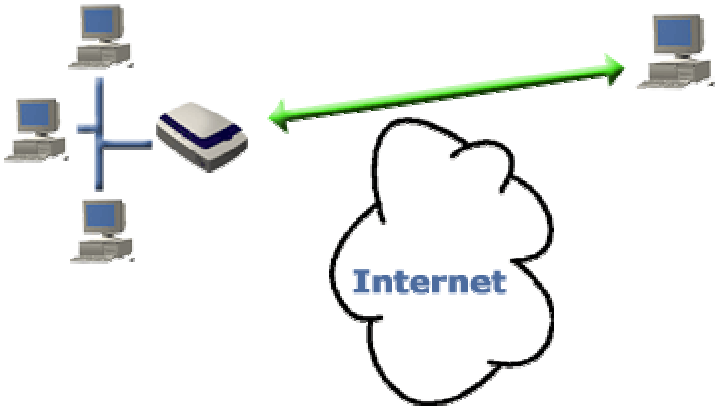


Figure 7.1 VPN tunneling using PPTP Server

PPTP client setup

The SnapGear PPTP client enables the SnapGear VPN Router to establish a VPN to a remote network running a PPTP server. This server will most likely be a Microsoft Windows server.

To begin setting up a SnapGear PPTP VPN Client, select **PPTP VPN Client** from the *VPN* menu. To create a new VPN connection, enter:

- A descriptive *name* for the VPN connection, which can provide an indication of the purpose of this connection.
- The remote PPTP *server IP address* to which to connect,
- A *username* and *password* you can use to login to the remote VPN, you may need to obtain this information from the system administrator of the remote PPTP server and,
- Optionally, the remote network's netmask.

Click **Add** – if the remote VPN is already up and running you can check **Start Now** to establish the connection immediately.

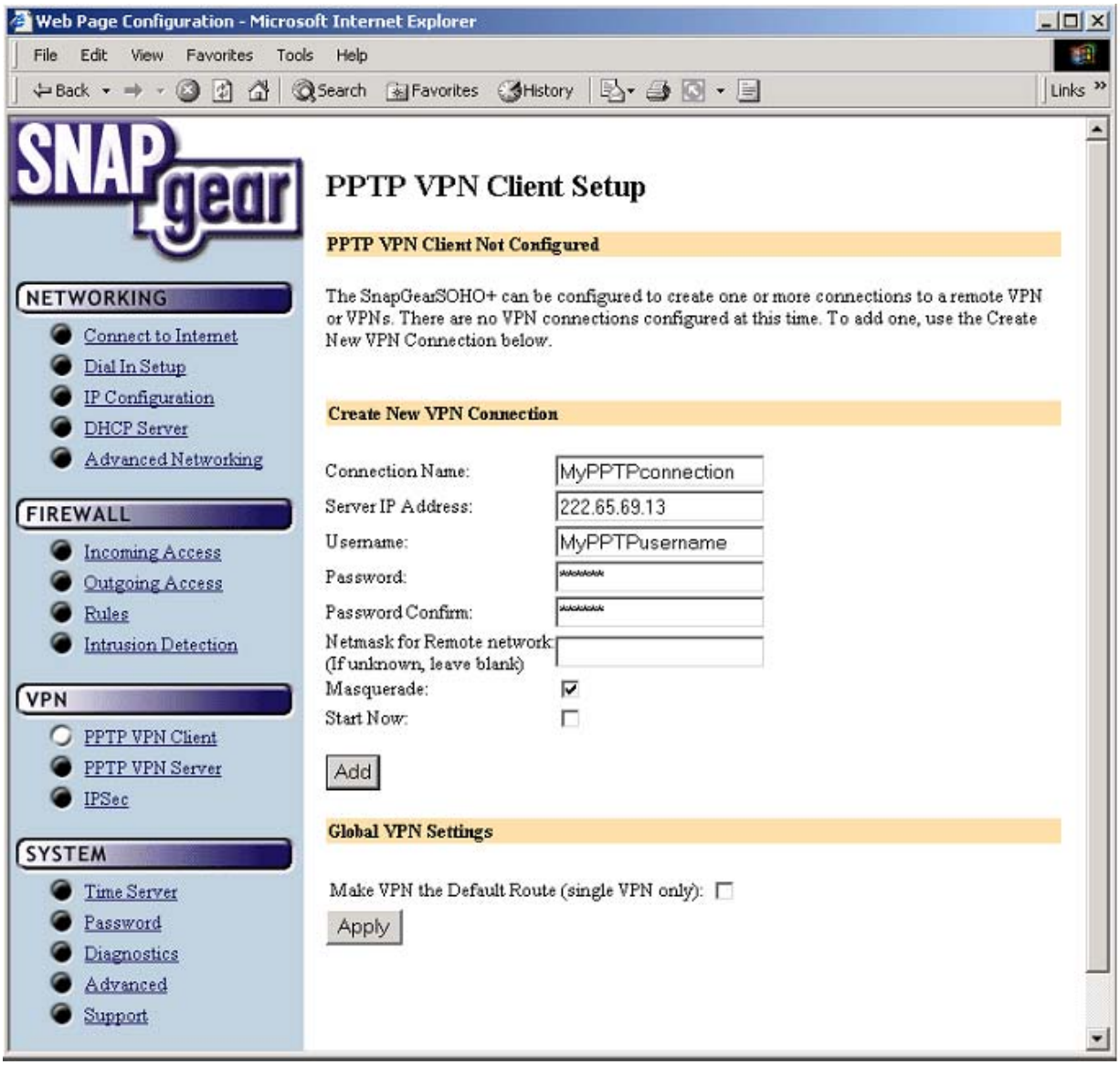


Figure 7.2 PPTP client configuration

The SnapGear VPN Router supports multiple VPN client connections and more can be added in the same manner as above. A VPN connection may be set as the default route for all network traffic by checking **Make VPN the Default Route** and clicking **Apply**. Note that this option is available only when the SnapGear VPN Router is configured with a single VPN connection only.

After a new VPN has been added, two new tables will be displayed in the *PPTP VPN Client* menu. *VPN Connection Status* provides information as to the *State* of the VPN (enabled/disabled) and the *Status* of the connection (up/down). The *VPN Configuration* table provides the ability to enable/disable the VPN, edit the VPN configuration, delete the VPN entry and edit advanced routing information.

PPTP server setup

The SnapGear VPN Router includes PPTP Server, a virtual private network server that supports up to forty simultaneous VPN tunnels, depending on the SnapGear VPN Router model. The SnapGear PPTP Server allows remote Windows clients to securely connect to the local network.

To setup a VPN connection:

- Enable and configure the PPTP VPN server.
- Set up VPN user accounts on the SnapGear VPN Router - with appropriate authentication security enabled.
- Configure the VPN clients at the remote sites. There is no need for any special software for the client. The SnapGear PPTP Server supports the standard PPTP client software now included in Windows 95/98, Windows ME, Windows XP, WinNT and Windows 2000. The VPN connection is simple to configure using the standard Dial-Up Networking software. The SnapGear PPTP Server is also compatible with Unix PPTP client software.
- Connect the remote VPN client.

More detailed instructions are provided in the following sections.

Enable and configure the PPTP VPN server

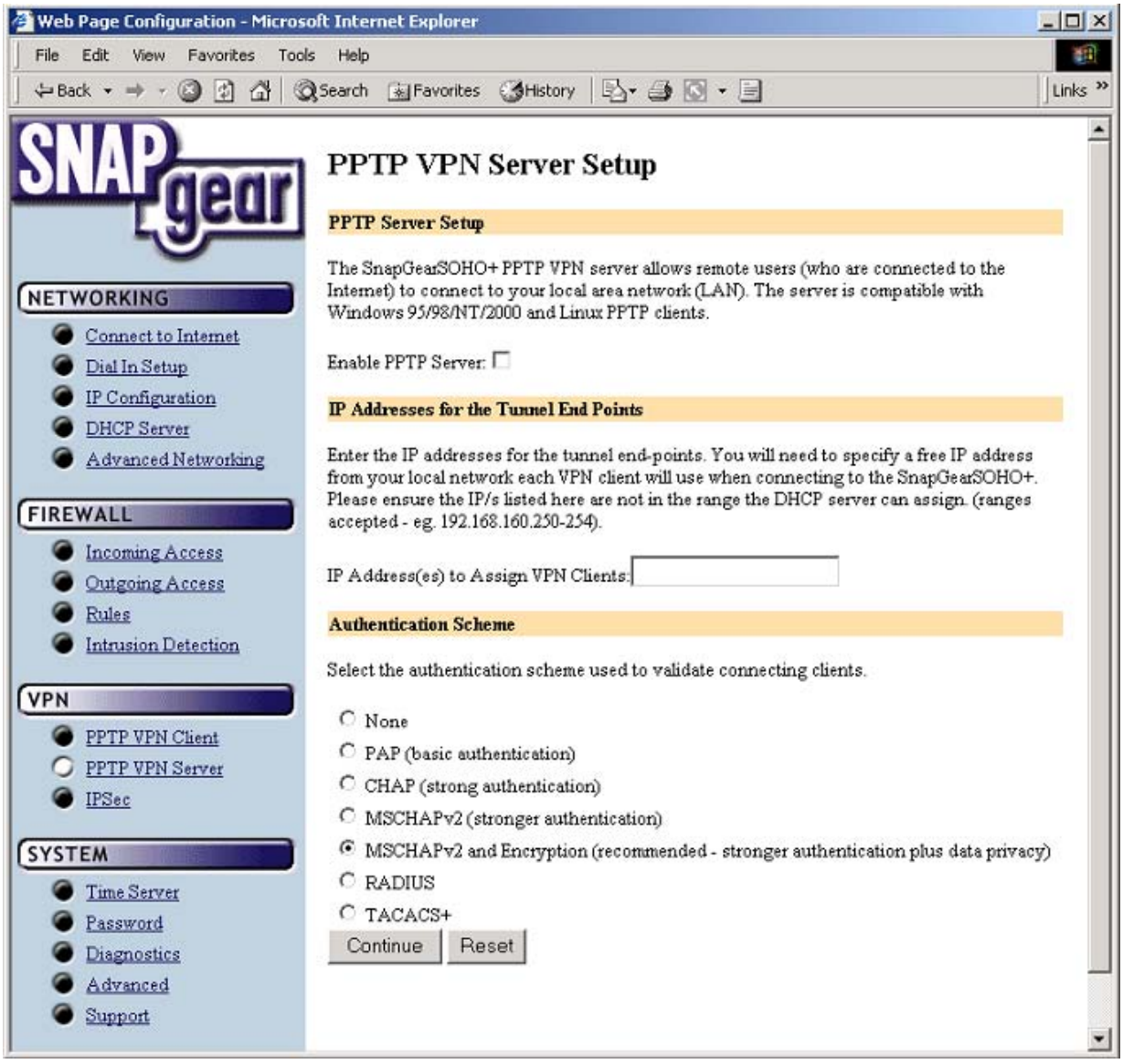

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
PPTP VPN Server Setup
PPTP Server Setup
The SnapGearSOHO+ PPTP VPN server allows remote users (who are connected to the Internet) to connect to your local area network (LAN). The server is compatible with Windows 95/98/NT/2000 and Linux PPTP clients.
Enable PPTP Server:
IP Addresses for the Tunnel End Points
Enter the IP addresses for the tunnel end-points. You will need to specify a free IP address from your local network each VPN client will use when connecting to the SnapGearSOHO+. Please ensure the IP/s listed here are not in the range the DHCP server can assign. (ranges accepted - eg. 192.168.160.250-254).
IP Address(es) to Assign VPN Clients:
Authentication Scheme
Select the authentication scheme used to validate connecting clients.
None
PAP (basic authentication)
CHAP (strong authentication)
MSCHAPv2 (stronger authentication)
MSCHAPv2 and Encryption (recommended - stronger authentication plus data privacy)
RADIUS
TACACS+
Continue
Reset

Figure 7.3 PPTP Server setup

To enable and configure SnapGear VPN Router's VPN server, select **PPTP VPN Server** from the **VPN** menu in the **SnapGear VPN Router Config Pages**. The table below describes the fields in the VPN Setup screen and the options available when enabling and configuring VPN access.

Field	Description
Enable PPTP Server	Check this box to enable PPTP connections to be established to your SnapGear VPN Router.
IP Addresses for the Tunnel End Points	Enter the IP addresses for the tunnel end-points. You will need to specify a free IP address from your local network that each VPN client will use when connecting to the SnapGear VPN Router. Please ensure that the IP addresses listed here are not in the range the DHCP server can assign. (Ranges are accepted - e.g. 192.168.160.250-254).
Authentication scheme	PPTP provides an authenticated communication tunnel between a client and a gateway by using a user ID and password. The authentication scheme you choose is the method by which the SnapGear VPN Router will challenge users who endeavor to establish a PPTP connection to the network. The remote client must be set up to use the selected authentication scheme. *MSCHAPv2* is the most secure. It uses encrypted passwords. SnapGear recommends the use of MSCHAPv2 plus data encryption as this keeps your data private as well as providing secure authentication. *CHAP* is less secure, and similarly *PAP* is even less secure, but more common. *RADIUS* and *TACACS+* make use of a remote authentication server on the local network. When selected you must enter the IP address of a server setup to use this scheme.

Configuring user accounts for VPN server

Once you have set up the VPN server, select **Continue** and you will be presented with a *PPTP VPN Server Accounts* screen.

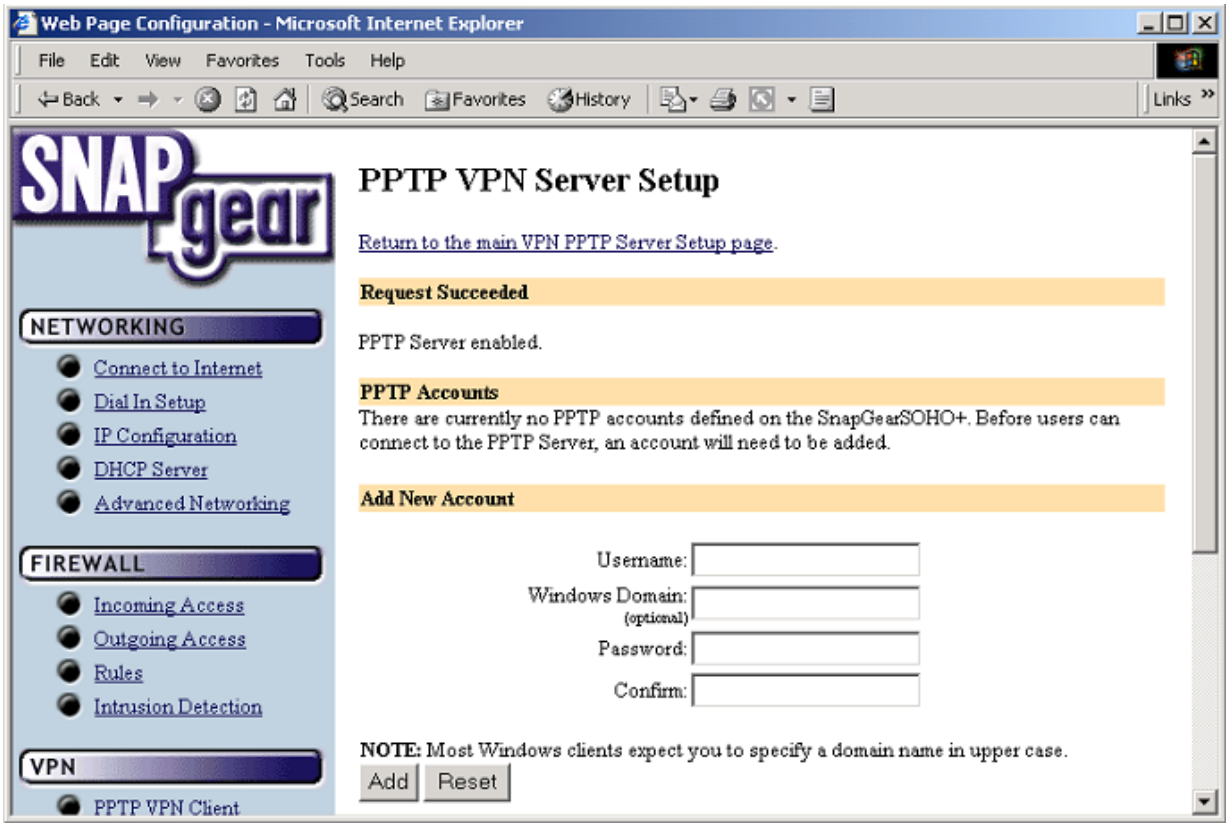


Figure 7.4 PPTP VPN Server Accounts screen

Before remote users can set up a VPN tunnel to the SnapGear VPN Router PPTP server, they must have user accounts set up. The field options in the **Add New Account** are detailed in the table below.

Field	Description
Username	This Username is required for VPN authentication only. The name selected is case-sensitive (for example *Jimsmith* is not the same as *jimsmith*). The Username can be the same as, or different to, the name set for dial-in access.
Windows Domain	Optional. Most Windows clients expect you to specify a domain name in upper case.
Password	Enter the password for the remote VPN user.
Confirm	Re-enter the password to confirm.

As new VPN user accounts are added, they are displayed on the updated *Account List*.

To modify the password of an existing account, **Select** the account in the *Account List* then enter **New Password** and **Confirm** in the **Delete or Change Password for the Selected Account** field.

To delete an existing account, **Select** the account in the *Account List* then check **Delete** in the **Delete or Change Password for the Selected Account** field.

If you request a change to a User Account and it is successful, the *PPTP VPN Setup* screen will be represented with the change noted. If the change request is unsuccessful, an error will be reported.

Configuring the remote VPN client

Having set up the SnapGear PPTP VPN server as described above, the remote VPN clients can now be configured to securely access the local network. You will need to supply the VPN client username and password. Your remote users will need these to access the SnapGear PPTP VPN from the remote site. These names may or may not be the same as your normal network username and password – and they will almost certainly be different from the username and password your remote users use when they log onto to their local ISP.

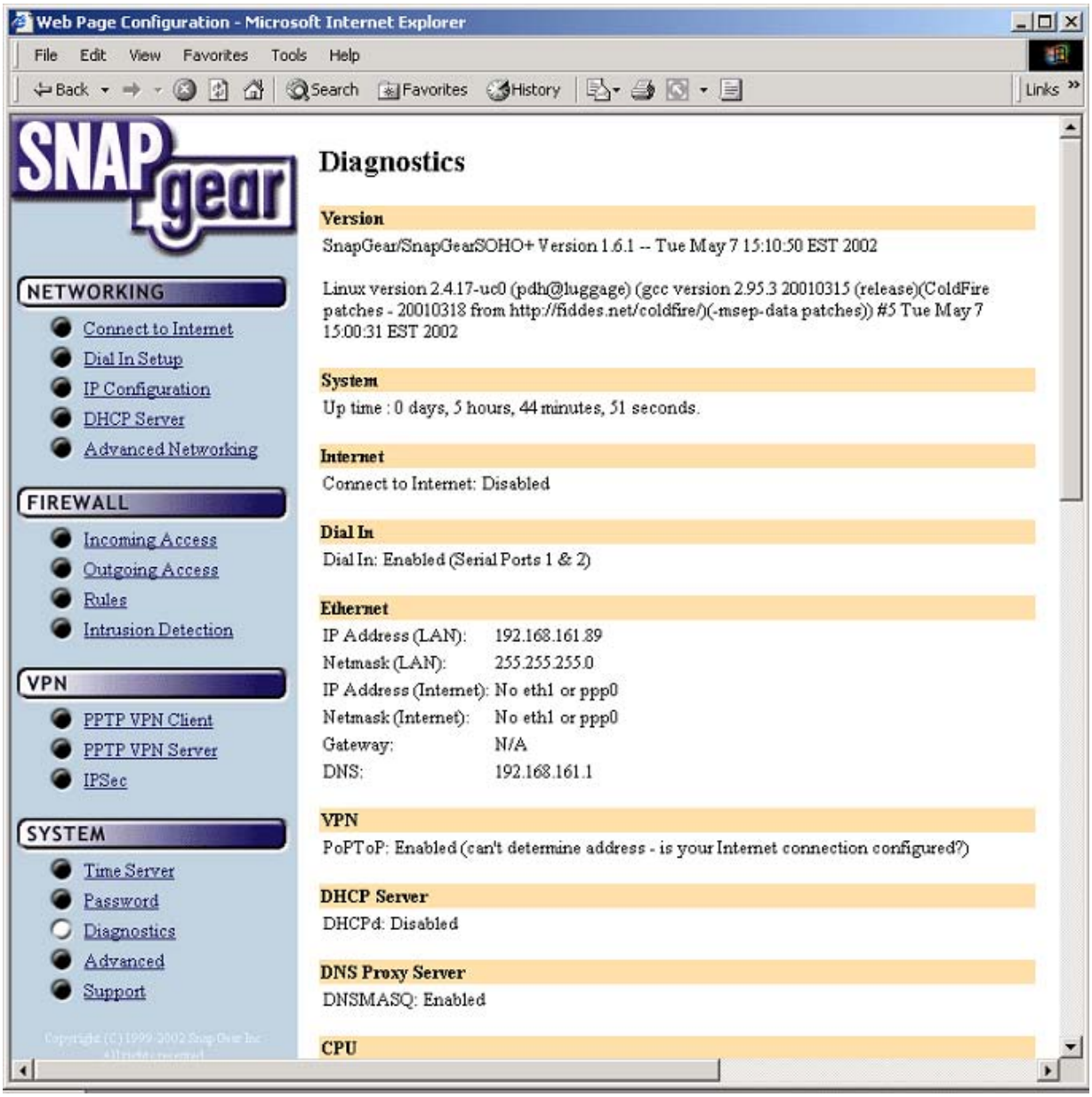


Figure 7.5 VPN PPTP IP address

Obtain the current IP address of the SnapGear VPN Router PPTP server. This address may change from time to time if your office network has an external DHCP server (i.e. your ISP dynamically assigns your an IP address). To determine the current SnapGear VPN Router's PPTP server IP address, select **Diagnostics** from the **System** menu in the main menu bar. The IP address will be displayed in the *VPN* field. Your remote users will need to know this *PPTP IP address* to be able to setup a VPN tunnel to the SnapGear VPN Router.

Check that the remote PC has a modem installed and that you have a local ISP account, i.e. ISP phone number and a username and password to log on to the ISP. (While it is common for remote users to be connected to the Internet by dial-out modem, the VPN connection can be set up over a cable modem, ADSL, ISDN or other Internet link).

Ensure that both VPN and Dial Up Networking (DUN) software is installed on your remote PC. If necessary, install the *Microsoft DUN update* (available on the *Installation* CD) and *VPN Client update.*

To create a VPN connection across the Internet, you must set up two networking connections. One connection is for your Internet access provider, and the other is for the VPN tunnel to your office network. Verify that there is already a networking connection established for the link to your local ISP.

Set up a new connection for the VPN connection. Your SnapGear VPN Router's PPTP server will operate correctly with the standard Windows PPTP clients in all versions of Windows. The following sections provide details for client setup in Windows 95/98, Windows NT, and Windows 2000. Setup instructions for Windows ME and Windows XP can be deduced from the information presented here and the Microsoft Windows documentation.

Windows 95 and Windows 98

From the Dial-Up Networking folder, double-click **Make New Connection**. Type **SnapGear VPN Router** or a similar descriptive name for the name of your new VPN connection.

From the **Select a device** drop-down menu, select the **Microsoft VPN Adapter** and click **Next**.

Enter the PPTP IP address of the SnapGear VPN Router VPN server in the **VPN Server** field – note that this may change from time to time if your ISP uses dynamic IP assignment. Click **OK** and then **Finish**.

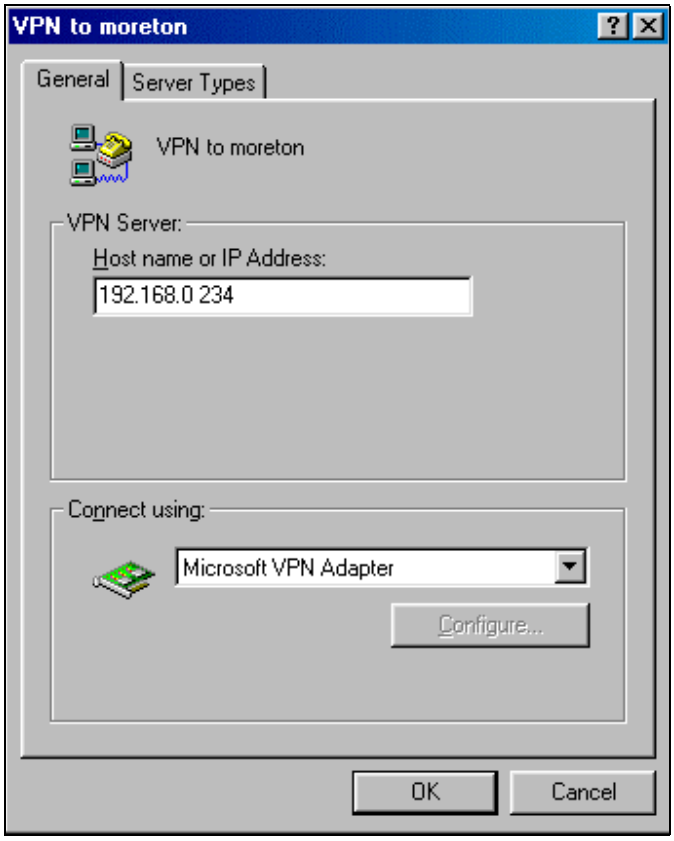


Figure 7.6 VPN client setup

Right-click on the new icon and select **Properties**.

Select the **Server Types** tab and check the **Log on to network**, **Enable software compression**, and **Require encrypted password** check boxes. Leave the other Advanced Options unchecked.

Select the **TCP/IP** network protocols from the **Allowed network protocols** list.

Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message will be returned.

Click **TCP/IP Settings**. Confirm that **Server Assigned IP Address, Server Assigned Name Server Address, Use IP Header Compression** and **Use Default Gateway on Remote Network** are all selected. Click **OK**.

Click **OK.** Your VPN client is now set up correctly.

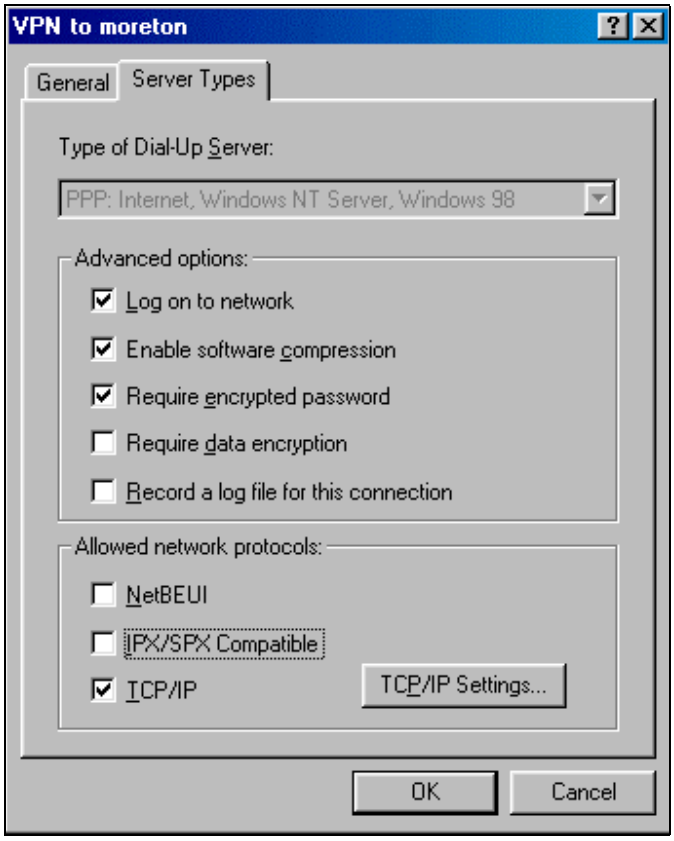


Figure 7.7 VPN client server settings

Windows NT

From the **Dial-Up Networking** dialog, click the **New** button. Select the **Basic** tab.

In the **Entry name** field, enter SnapGear VPN Router or a similar descriptive name and click **Next**.

Enter the SnapGear VPN Router's *PPTP IP address* into the **Phone Number** field.

Warning: *Note that this IP address may change from time to time if your ISP uses dynamic IP assignment.*

In the **Dial Using** dialog box, select RASSPPTPM (VPN1) and click **Next**.

Click **More** and select **Edit entry** then **Modem properties** from the menu.

Select the **Server** tab.

Select **TCP/IP** only.

Warning: *Do not select NetBEUI or IPX. If an unsupported protocol is selected, an error message will be returned.*

Select the **Security** tab.

Select **Accept only Microsoft encrypted authentication**. Click **OK**. Your VPN client is now set up correctly.

Windows 2000

To set up VPN access, you first need to set up a Dial Up Networking account to access the Internet. Once you have done this, you are ready to begin.

The first thing you need to do is log in as Administrator on your PC. Once logged in, from the **Start** menu, select **Settings** and then **Network and Dial-up Connections.**

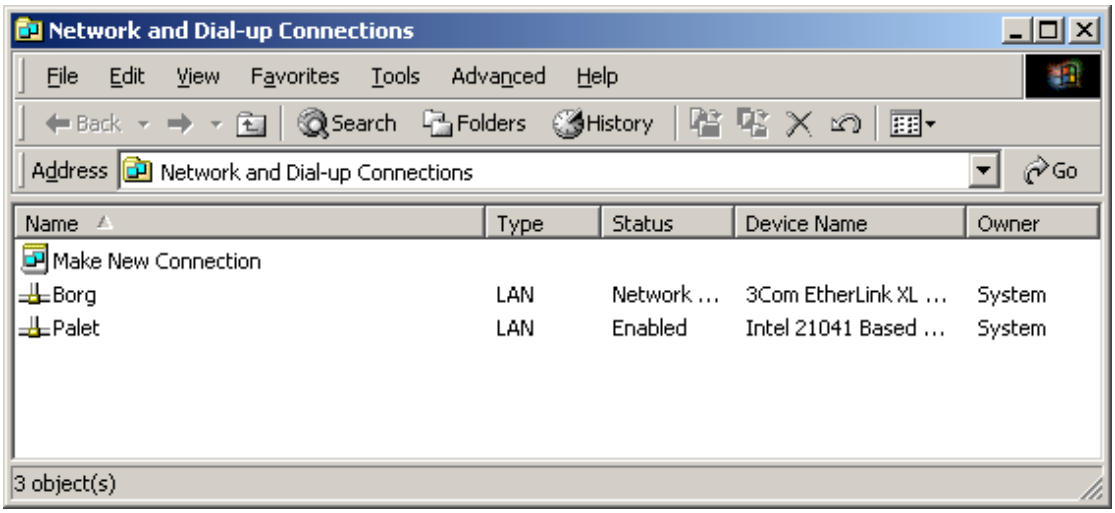

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Name Type Status Device Name Owner
Make New Connection
Borg LAN Network ... 3Com EtherLink XL ... System
Palet LAN Enabled Intel 21041 Based ... System
3 object(s)

Figure 7.8 Network and Dial-up Connections

To set up your VPN account, double-click on **Make New Connection** then click **Next** on the first window of this wizard, which will bring up the **Network Connection Type** window.

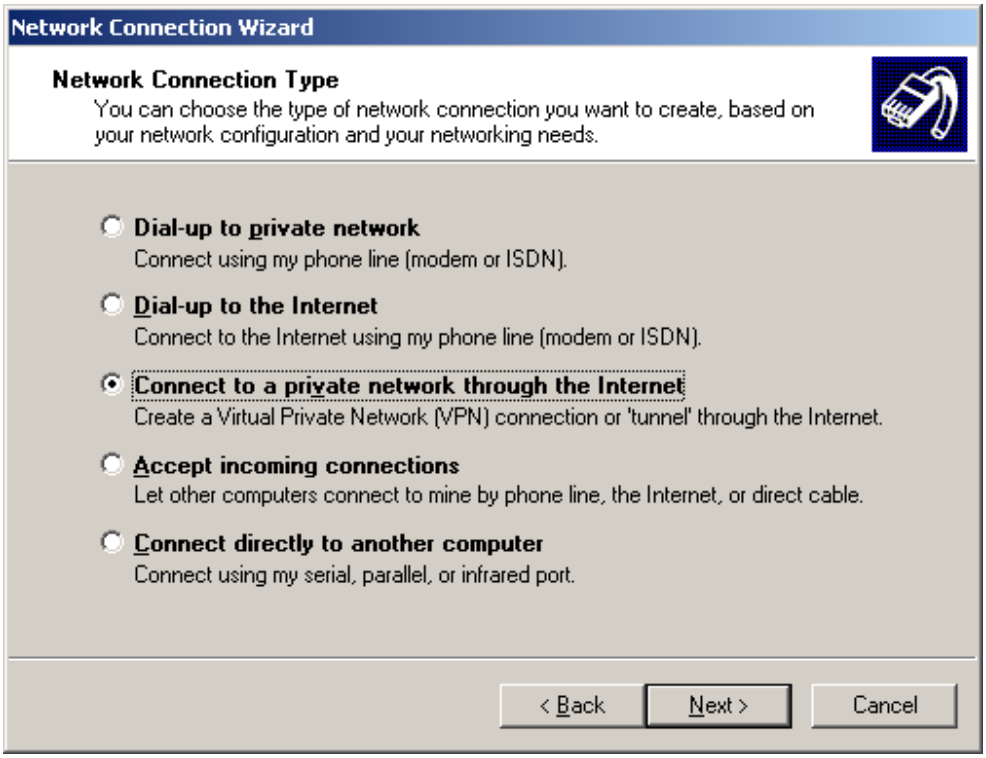

Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

Figure 7.9 Network Connection Type

Select **Connect to a private network through the Internet** and click **Next**. This displays the Destination Address window.

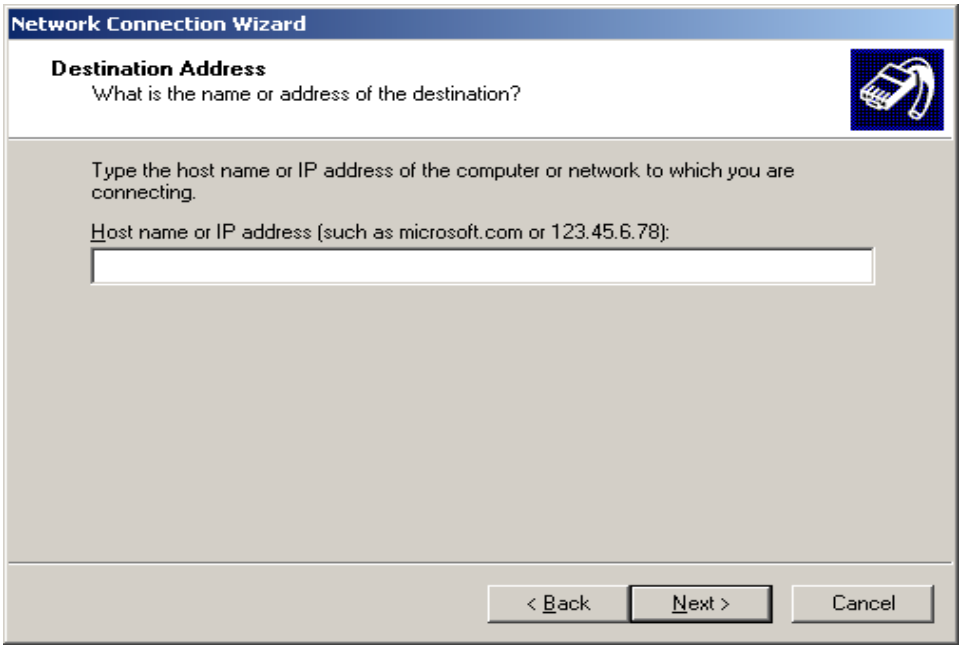

Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
< Back
Next >
Cancel

Figure 7.10 Destination Address

Enter the SnapGear PPTP server's IP address and click **Next**. Select the **Connection Availability** that you require on the next window and click **Next**, which will display the final window in this wizard.

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Virtual Private Connection
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

Figure 7.11 Completing the Network Connection Wizard

Enter an appropriate name for your connection and click **Finish**. Your VPN client is now set up correctly.

Connecting the remote VPN client

Firstly, connect to the Internet using the network connection to your ISP.

After the connection to your ISP has been authenticated, select the connection for the SnapGear VPN Router VPN.

For *Windows 95/98/2000*, enter the username and password given to you by the SnapGear VPN Router's VPN administrator and click **Connect**.

For *Windows NT*, click **Dial** and enter the username and password given to you by the SnapGear VPN Router's VPN administrator.

After you have been authenticated to the network, you can check your e-mail, use the office printer, access shared files and browse the network – as if you were physically connected to the LAN.

To disconnect the VPN tunnel connection to the remote SnapGear VPN Router:

- From the desktop, double-click **My Computer** then **Dial-Up Networking** and select the phonebook entry for the SnapGear VPN Router VPN.
- For *Windows 95/98/2000* click the **Disconnect** button
- For *Windows NT*, click the **Hang up** button

You may then disconnect from the Internet.

IPSec Setup

The SnapGear VPN router supports IPSec tunnels as well as PPTP tunnels. To setup your VPN using IPSec, select IPSec from the VPN menu:

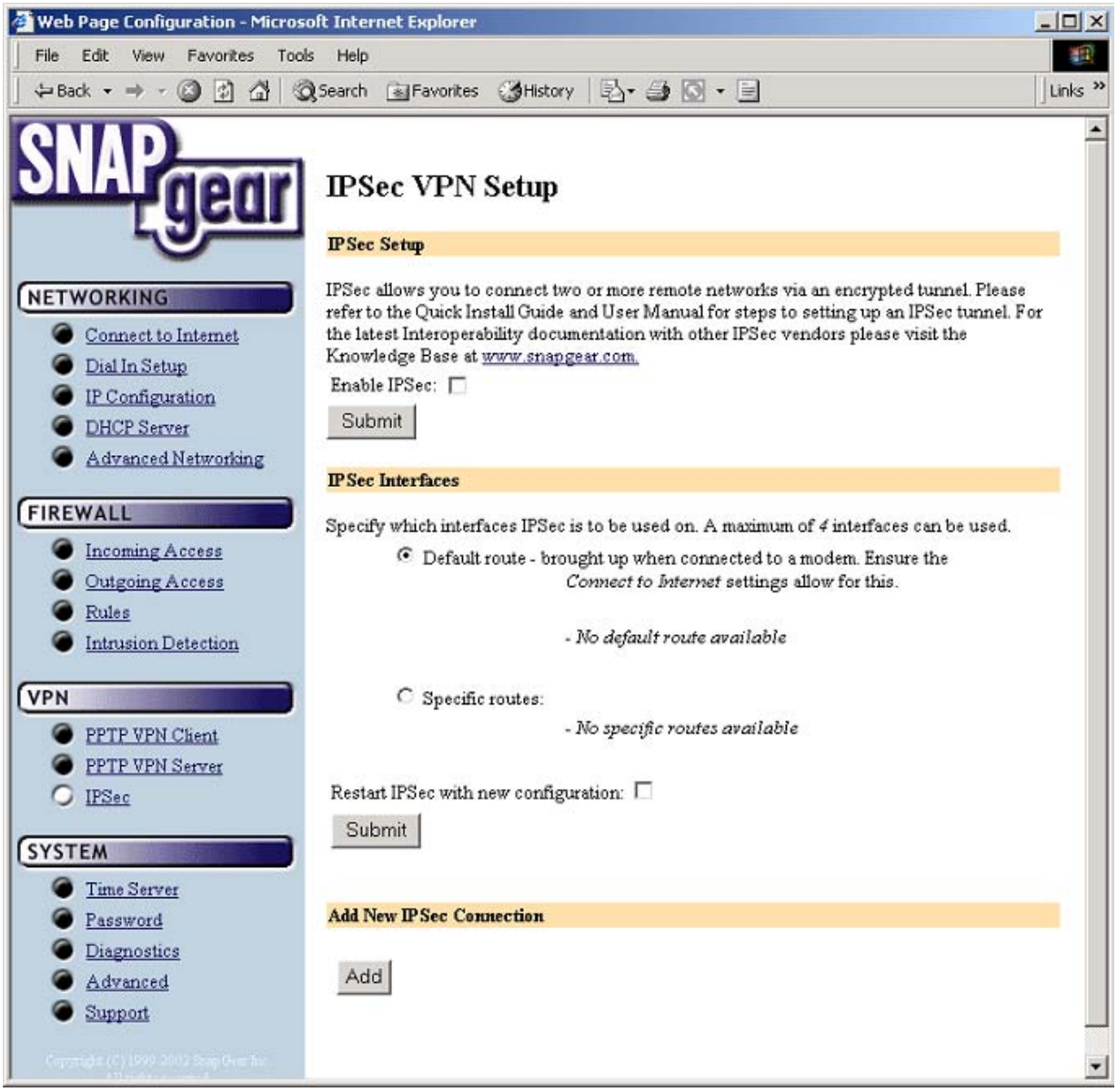
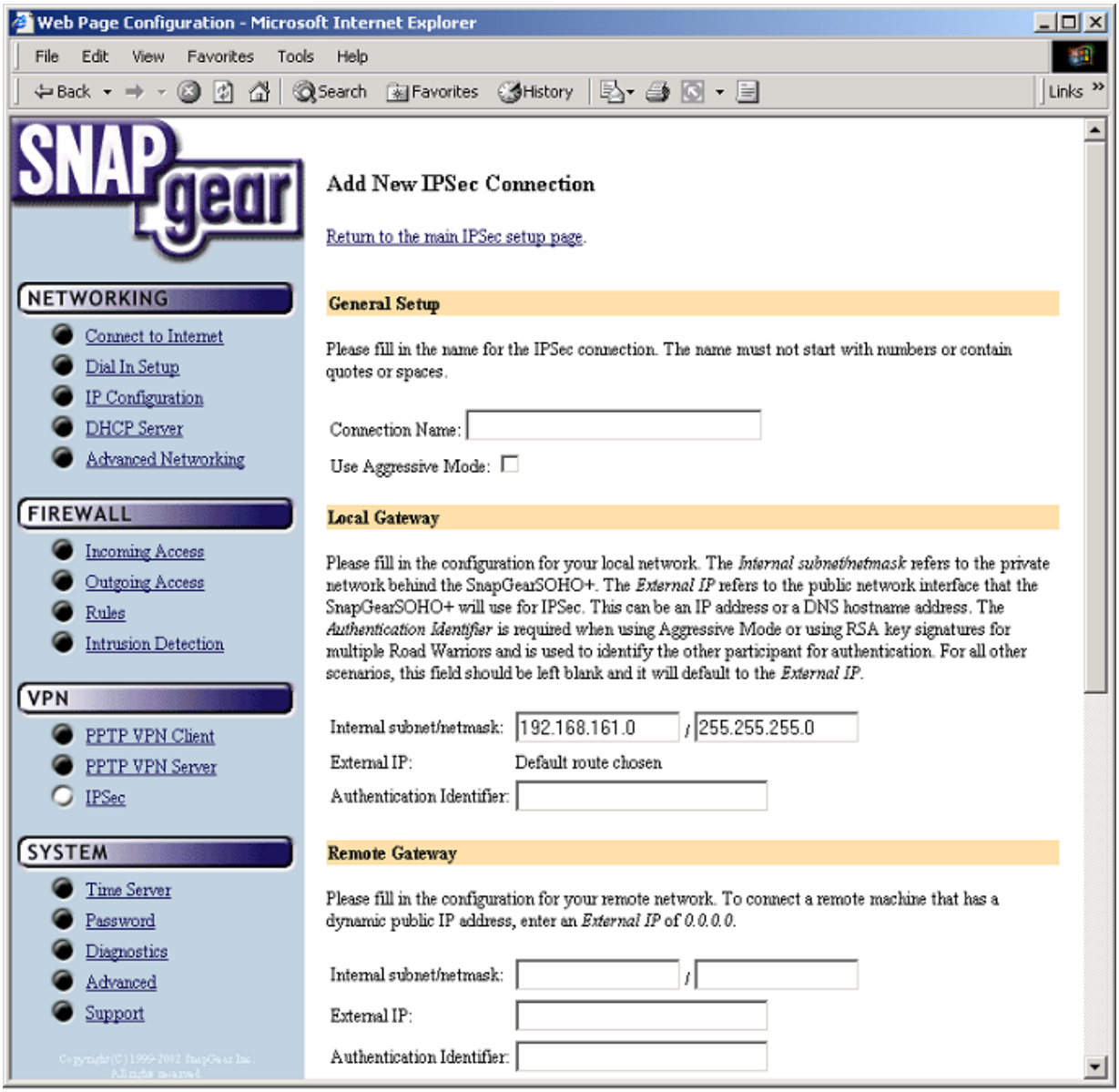

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
IPSec VPN Setup
IPSec Setup
IPSec allows you to connect two or more remote networks via an encrypted tunnel. Please refer to the Quick Install Guide and User Manual for steps to setting up an IPSec tunnel. For the latest Interoperability documentation with other IPSec vendors please visit the Knowledge Base at www.snapgear.com.
Enable IPSec:
Submit
IPSec Interfaces
Specify which interfaces IPSec is to be used on. A maximum of 4 interfaces can be used.
Default route - brought up when connected to a modem. Ensure the Connect to Internet settings allow for this.
- No default route available
Specific routes:
- No specific routes available
Restart IPSec with new configuration:
Submit
Add New IPSec Connection
Add

Figure 7.12 IPSec Setup

Enable IPSec by clicking the **Enable IPSec** box underneath the **IPSec Setup** title. Then click **Submit**.

Enable the interface on which you want to use IPSec. This may be the default gateway or a ppp interface for ADSL and cable modems, or "eth1" if the SnapGear VPN Router is connected to a router before connecting to the Internet. Then click **Submit**.

To add a new IPSec connection click on **Add** under **Add New IPSec Connection**.


Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Add New IPSec Connection
Return to the main IPSec setup page.
General Setup
Please fill in the name for the IPSec connection. The name must not start with numbers or contain quotes or spaces.
Connection Name:
Use Aggressive Mode:
Local Gateway
Please fill in the configuration for your local network. The Internal subnet/netmask refers to the private network behind the SnapGearSOHO+. The External IP refers to the public network interface that the SnapGearSOHO+ will use for IPSec. This can be an IP address or a DNS hostname address. The Authentication Identifier is required when using Aggressive Mode or using RSA key signatures for multiple Road Warriors and is used to identify the other participant for authentication. For all other scenarios, this field should be left blank and it will default to the External IP.
Internal subnet/netmask: 192.168.161.0 / 255.255.255.0
External IP: Default route chosen
Authentication Identifier:
Remote Gateway
Please fill in the configuration for your remote network. To connect a remote machine that has a dynamic public IP address, enter an External IP of 0.0.0.0.
Internal subnet/netmask: /
External IP:
Authentication Identifier:

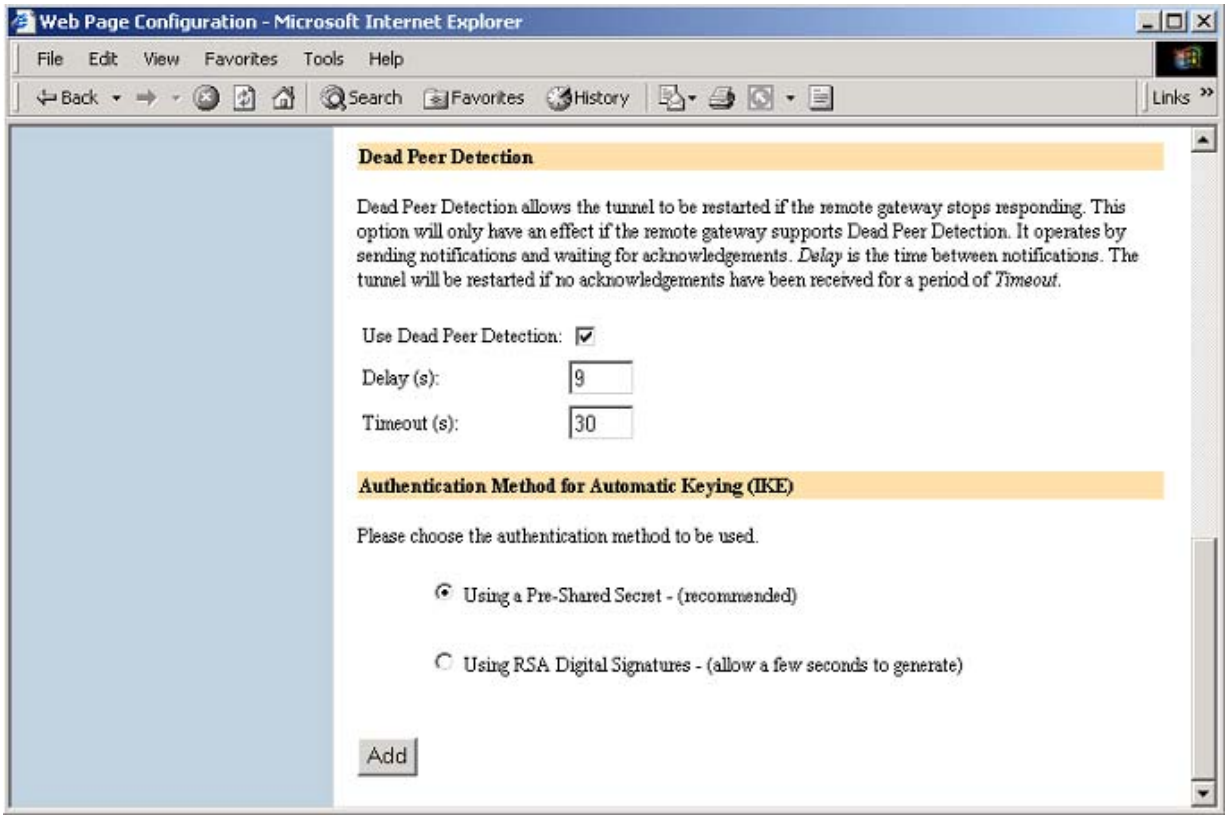

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
Dead Peer Detection
Dead Peer Detection allows the tunnel to be restarted if the remote gateway stops responding. This option will only have an effect if the remote gateway supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements. Delay is the time between notifications. The tunnel will be restarted if no acknowledgements have been received for a period of Timeout.
Use Dead Peer Detection:
Delay (s): 9
Timeout (s): 30
Authentication Method for Automatic Keying (IKE)
Please choose the authentication method to be used.
Using a Pre-Shared Secret - (recommended)
Using RSA Digital Signatures - (allow a few seconds to generate)
Add

Figure 7.13 Add new IPSec Connection

Enter a descriptive name for the connection in the **Connection Name** field.

Choosing to connect with *Aggressive Mode* increases interoperability with third party IPSec servers that only support aggressive mode connections.

Enter the local gateway settings. The *Internal subnet/netmask* refers to the private network behind the SnapGear VPN Router. The *External IP* refers to the public-network interface that the SnapGear VPN Router will use for IPSec. The *Authentication Identifier* is required when using RSA key signatures for multiple Road Warriors and is used to identify the other participant during authentication. If this field is left blank, the Authentication Identifier defaults to the External IP. *Nexthop* refers to the next-hop gateway IP address to the public network, which is not normally required and may be left blank. This option is only available if you've chosen a specific route. It is recommended that you use the default route. Enter the remote gateway settings. To connect to/from a remote machine that does not have a fixed IP address, (e.g. a Road Warrior), enter an *External IP* of *0.0.0.0* only.

Dead Peer Detection allows the tunnel to be restarted if the remote gateway stops responding. This option will only have an effect if the remote gateway supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements. *Delay* is the time between notifications. The tunnel will be restarted if no acknowledgements have been received for a period of *Timeout*.

The recommended keying used in IPSec is *Automatic Keying* (IKE). The default and recommended method of authentication is through a *Pre-Shared Secret*. A *Pre-Shared Secret* should be at least 24 characters long, and should be a phrase you can remember easily but would be difficult for others to guess. Authentication can also be achieved using RSA Digital Signatures.

Click **Add** to complete the IKE setup.

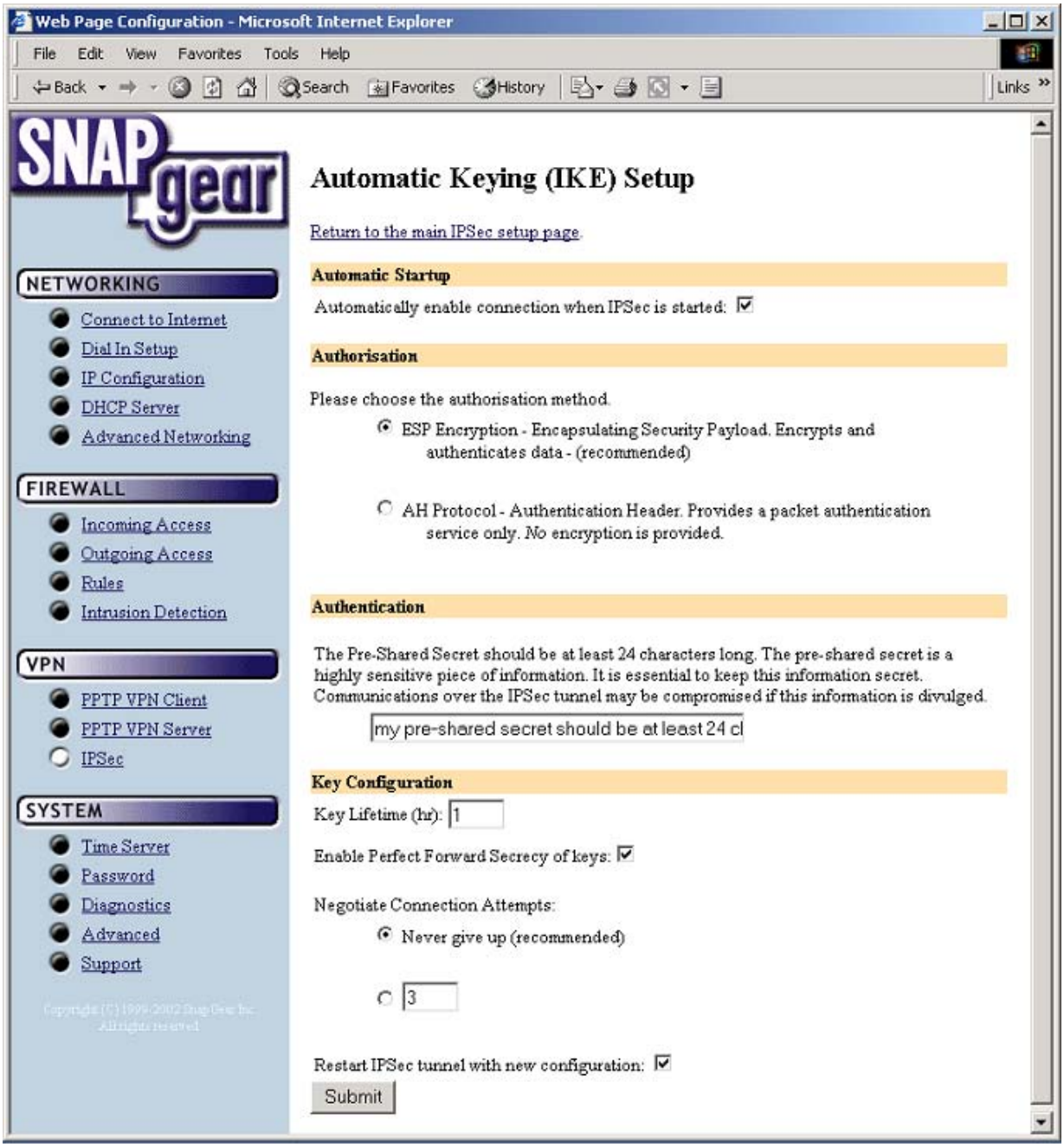

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Incoming Access
Outgoing Access
Rules
Intrusion Detection
VPN
PPTP VPN Client
PPTP VPN Server
IPSec
SYSTEM
Time Server
Password
Diagnostics
Advanced
Support
Automatic Keying (IKE) Setup
Return to the main IPSec setup page.
Automatic Startup
Automatically enable connection when IPSec is started:
Authorisation
Please choose the authorisation method.
ESP Encryption - Encapsulating Security Payload. Encrypts and authenticates data - (recommended)
AH Protocol - Authentication Header. Provides a packet authentication service only. No encryption is provided.
Authentication
The Pre-Shared Secret should be at least 24 characters long. The pre-shared secret is a highly sensitive piece of information. It is essential to keep this information secret. Communications over the IPSec tunnel may be compromised if this information is divulged.
my pre-shared secret should be at least 24 cl
Key Configuration
Key Lifetime (hr): 1
Enable Perfect Forward Secrecy of keys:
Negotiate Connection Attempts:
Never give up (recommended)
3
Restart IPSec tunnel with new configuration:
Submit

Figure 7.14 Automatic Keying Setup

Click **Submit** to add the new IPSec tunnel after selecting the appropriate *Automatic Startup*, *Authorization, Authentication*, and *Key Configuration*.

Warning: *The pre-shared secret must be entered identically at each end of the tunnel. The IPSec tunnel will fail to connect if the pre-shared secret is not identical at both ends.*

The pre-shared secret is a highly sensitive piece of information. It is essential to keep this information secret. Communications over the IPSec tunnel may be compromised if this information is divulged.

Automatic keying provides a mechanism for regularly changing the cryptographic keys used by the IPSec tunnel. This regular key change results in enhanced security, since if an enemy gets one key only messages between the previous re-keying and the next are exposed. The **Key Lifetime** is the time between consecutive re-keying events, that is, the lifetime of a key. Shorter values offer higher security at the expense of the computational overhead necessary to calculate new keys. The default value of 1 hour is recommended.

Checking the **Enable Perfect Forward Secrecy of keys** box means that an attacker who acquires the SnapGear VPN Router's long-term key (i.e. the *pre-shared secret* or *RSA Signature Key Private Section*) can:

- *Neither* read previous messages which he may have archived
- *Nor* read future messages without performing additional successful attacks

Perfect forward secrecy of keys provides the maximum security and is the recommended setting.

IPSec Interoperability

Please see the Support Knowledge Base (http://www.snapgear.com/knowledgebase.html) on the SnapGear Web Site (http://www.snapgear.com/) for detailed information on successfully establishing IPSec tunnels between your SnapGear VPN Router and other vendors' equipment.

8. System

Time Server

The SnapGear VPN Router can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP Time Server ensures that the SnapGear VPN Router's clock (in UTC) will be accurate soon after the Internet connection is established. If NTP is not used, the system clock will be set randomly when the SnapGear VPN Router starts up.

To set the system time using NTP, select the **Set Time** check box on the *NTP Server Configuration* page and enter the IP address of the time server in the **Remote NTP Server** field.

Password

The SnapGear VPN Router's password is used to restrict access to the SnapGear VPN Router's Configuration web pages and the SnapGear VPN Router itself. A potential security issue may be introduced by having a network-connected SnapGear VPN Router accessible, using the factory default password. To prevent this, the SnapGear VPN Router's password must be changed when Setup Wizard is run or the Configuration web pages are accessed for the first time. The SnapGear VPN Router's password can be changed at any time through the Configuration web pages by clicking **Password** in the **System** menu.

The SnapGear VPN Router's password is the 'key' to the security of your network; it is essential to keep it secret. SnapGear recommends choosing a password that is easy for you to remember but hard for unauthorized people to guess.

Note that:

- The *username* field will be ignored - there is no username.
- The SnapGear VPN Router factory default password is: *default.*

Diagnostics

If you are experiencing problems with your SnapGear VPN Router, diagnostic information is provided on the SnapGear VPN Router's Configuration web pages. To access this information, from the **System** menu, click **Diagnostics**. Advanced network diagnostics can be viewed by selecting the **Networking** menu, then **Advanced Networking**.

Advanced

Options on the *Advanced* page are intended for network administrators and advanced users **only**. Altering the advanced configuration settings may render your SnapGear VPN Router inoperable.

The *System Log* contains debugging information that may be useful in determining whether all SnapGear VPN Router's services are operating correctly. The SnapGear VPN Router also provides the option of redirecting log output to a remote machine that is using the *syslog* protocol. This can be enabled by selecting **Enable Remote Logging**, entering the IP address of the remote machine and clicking **Apply**.

Flash upgrade

The SnapGear VPN Router's firmware can be updated with newer versions available from the SnapGear web site (http://www.snapgear.com/downloads.html). These come in the form of binary image files (*.bin*) that can be transferred from a PC on the local network directly into the SnapGear VPN Router's flash memory. To perform flash upgrades, the SnapGear VPN Router must already be configured on the local network with an IP address.

Flash upgrades can be performed using the configuration web pages. To do this, click **Advanced** then **Flash Upgrade** and enter the IP address of the PC with the binary image and the appropriate filename. A TFTP server must be running on the machine that is hosting the file.

While the SnapGear VPN Router is being upgraded, its front panel LEDs will flash in an in-and-out pattern. The SnapGear VPN Router retains its configuration information with the new firmware.

***Warning**: Should the flash upgrade be interrupted in any manner (eg. power down), the SnapGear VPN Router will stop functioning and will be unusable until its flash is reprogrammed at the factory. User care is advised.*

RESET button

The simplest method of clearing the SnapGear VPN Router's stored configuration information is to push the reset button on the back of the SnapGear VPN Router box. It is the small hole between the serial ports and ethernet ports. A bent paper clip is the simplest method.

Pushing this button will clear all stored configuration back to the SnapGear VPN Router's factory defaults. It will also reboot the SnapGear VPN Router.

9. Technical Support

Under the *System* menu, there is a menu option outlining support information for your SnapGear VPN Router.

This page provides some basic troubleshooting tips, contact details for SnapGear Support, and links to the SnapGear Knowledge Base.

Web Page Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
SNAPgear
NETWORKING
Connect to Internet
Dial In Setup
IP Configuration
DHCP Server
Advanced Networking
FIREWALL
Technical Support
Here are some easy options for gaining technical support:
1. Make sure that you have the latest firmware. New firmware is made available regularly be sure to read the Release Notes for important information about the features of the new firmware and any upgrade issues.
2. Please try the Knowledge Base. Many common problems can be solved here.
3. Have you tried searching the site? The search will look in the Knowledge Base and other areas of the site.
4. If your question is not answered here then please try contacting your reseller, or if you bought directly from SnapGear then submit an e-mail to support@snapgear.com and attach the SnapGearSOHO's Technical Support Report.
5. In the USA you may call 801-282-8498 between 9am and 5pm MST.
6. In Asia/Pacific you may call 617-34352888 between 9am and 5pm Australia EST.
Internet

Figure 9.1 Technical Support

The **Technical Support Report** page is an invaluable resource for the SnapGear Technical Support Staff to analyze problems with your SnapGear VPN Router. The information on this page gives the Support Staff important information about any problems you may be experiencing.

Should you experience a fault with your SnapGear VPN Router, please attach the **Technical Support Report** to your support request.

Appendix A – LED Status Patterns

The table below shows the various LED illumination combinations that serve to show possible error conditions. In each case, the LEDs indicated will be on and steady, unless otherwise noted, and all other LEDs will be off. The Power and System LEDs do not form part of the grouping of status-indicating LEDs. Where the action indicates that you should contact your dealer, please take note of the LED pattern to facilitate faster response and recovery action.

LED Pattern	Status	Action
VPN	Memory failure	Contact your dealer
COM2	Console device cannot initialize	Contact your dealer
All LEDs on	In recovery mode, usually from a bad Flash image. While the reset button is held in this will be the LED pattern.	
VPN & Internet Link	Cannot load static data into memory, probably memory and/or Flash problem	Contact your dealer
COM2 & Internet Link	Cannot load SBSS, probably memory and/or Flash problem	Contact your dealer
Online	Memory exception	Contact your dealer